RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

To:	Amar Patel (Sheriff), Gregory.Wing@ic.fbi.gov, Michael.Tomasiello (Chicago Police), Douglas Maclean (Sheriff)
Cc:	Adnan Memon (Sheriff), Douglas Maclean (Sheriff), Michael.Tomasiello (Chicago Police), Amar Patel (Sheriff)
Sent:	December 31, 1600 6:00:00 PM CST
Received:	June 24, 2020 2:24:57 PM CDT

[Krebs on Security] 'BlueLeaks' Exposes Files from Hundreds of Police Departments

From: KrebsOnSecurity Mailing List <bk@krebsonsecurity.com>
To: bk@krebsonsecurity.com
Sent: June 21, 2020 11:33:26 PM CDT
Received: June 21, 2020 11:35:18 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Krebs on Security has posted a new item.

Hundreds of thousands of potentially sensitive files from police departments across the United States were leaked online last week. The collection, dubbed "BlueLeaks" and made searchable via a new website by the same name, stems from a security breach at a Texas web design and hosting company that maintains a number of state law enforcement data-sharing portals online.

https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

Please use the link above to continue reading this posting.
* *

Survey Report: SANS Automation and Integration Survey

The goal of the Automation and Integration Survey is to quantify automation experiences to better understand how organizations can maximize their security investment while improving operations through automation efforts. The survey looked at what automation activities have been successful, why they were successful, and how organizations approached their automation activities to achieve meaningful results. Discover the trends and themes that emerged from this year's survey.

Download Now:
https://www.krebsonsecurity.com/domaintools/
* *

You received this e-mail because you asked to be notified when new updates are posted.

Best regards,

BrianKrebs
https://krebsonsecurity.com

P.S. You may manage your subscription here:
https://krebsonsecurity.com/subscribe/

OODA Loop Daily Pulse | 06/22/2020

From: OODA Loop <loop@ooda.com>
To: myron.weres@cookcountyil.gov, Myron Weres (Sheriff) <Myron.Weres@cookcountyil.gov>

Sent: June 22, 2020 9:01:15 AM CDT
Received: June 22, 2020 9:01:26 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

OODA ORIGINAL ANALYSIS

The latest original analysis and research available exclusively at OODALoop.com.

- **OODA Video: The Technologies of AI Security and Ethics**
- **OODA Network Interview: Dr. Gaurav Banga**

CYBER THREAT BRIEF

The latest cyber threat and risk news.

Google Yanks 106 'Malicious' Chrome Extensions

On Thursday, Google removed over 100 Chrome browser extensions that it found to be malicious, after reports that they were being used to siphon sensitive user data. Google also published the research behind the apps, in which Awake Security alleges millions of Chrome users have been targeted by threat actors. | **(Read More)**

Hacker arrested for stealing, selling PII of 65K hospital employees

Justin Sean Johnson, a 29-year-old man from Michigan, was arrested earlier this week for his

involvement in a 2014 hack of the health care provider University of Pittsburg Medical Center (UPMC). Johnson allegedly executed the attack and stole personally identifiable information and W-2 information of over 65,000 employees. Johnson is | **(Read More)**

Data from 200 US police departments & fusion centers published online

On Friday, an activist group that describes itself as a transparency collective published 296GB of data that appears to have been stolen from US law enforcement agencies and fusion centers. The massive data leak has been named BlueLeaks and was published by the group Distributed Denial of Secrets (DDoSecrets). The | **(Read More)**

Facebook Pulls Trump Campaign Ad Featuring Nazi Symbol

Facebook has made the decision to remove advertising for Donald Trump's re-election campaign because it featured a symbol that is heavily associated with Nazi Germany. The advertisements, which stated that left-wing activists he calls Antifa should be branded a terrorist organization, had an inverted red triangle. The inverted red triangle | **(Read More)**

Sophisticated State-Backed Attack Rocks Australia

Today, Australian Prime Minister Scott Morrison warned of a high threat state-sponsored cyber espionage campaign targeting both the government and private sector within the country. Morrison urged domestic organizations to improve their security practices such as enabling multi-factor authentication and installing released patches immediately. Morrison also stated that the threatening | **(Read More)**

GLOBAL RISK BRIEF

The latest global risk news.

As virus spikes, Pakistan says there's no choice but to open

In Pakistan, COVID-19 is spreading at one of the fasted rates in the world, and hospitals can't keep up. Health care facilities have been turning away patients as they continue to receive hundreds of COVID-19 patients per day. However, the government is moving forward with opening up the country due | **(Read More)**

Brazil becomes second country to pass 50,000 deaths

Brazil has recently become the second country to reach more than 50,000 COVID-19 related deaths, following the US in terms of the highest infection and death rates. This milestone comes amid growing political tension and just a few days after officials confirmed more than one million COVID-19 infections within the | **(Read More)**

A new threat to global trade, Exhausted crews want off cargo ships now

Global trade is facing another economic crisis due to the COVID-19 pandemic, as seafarers stranded for months due to port closures could refuse to keep working. Many cargo ship crew extended their

contracts by several months to continue to supplies of food, fuel, and medicine flowing around the world during | **(Read More)**

China charges 2 Canadians with spying in Huawei-linked case

Today, two Canadians detained in China were charged with spying in a bid to step up pressure on Canada to drop the US's extradition request for prominent Huawei employee who is currently serving house arrest in Vancouver. One of the Canadians, Michael Kovrig, was charged by china on suspicion of | **(Read More)**

Coronavirus was already in Italy by December, waste water study finds

Italian officials say that the COVID-19 virus was present in the country in December, after the National Institute of Health stated that water from Milan and Turin showed genetic traces of the virus on December 18. This adds to the increasing amount of evidence that the virus has been circulating | **(Read More)**

TECHNOLOGY BRIEF

The important technology news.

Nextdoor eliminates its Forward to Police program

Nextdoor, a neighborhood social networking app has announced that they are discontinuing their Forward to Police feature that allowed users to send message board posts directly to the local police department. The platform has been controversial lately for how it handles communications with law enforcement and racism among members of | **(Read More)**

Robot Divers Could Use Artificial Intelligence To Save Coral Reefs

A National Oceanic and Atmospheric Administration organization claims that humans will not be able to save the coral reefs dying at an alarming rate across the globe. In optimal conditions, human divers can still only spend three to four hours per day working underwater in restoration efforts. Tom Moore, program | **(Read More)**

NIH Partners with Israeli Startup to Generate Synthetic COVID-19 Data

On Thursday, the National Institutes of Health announced a new partnership with Israeli startup MDClone. The collaboration is an attempt to generate computationally derived synthetic data from aggregated clinical health data. The data will be utilized to advance COVID-19 research. This is a new development in the NIH's National COVID | **(Read More)**

Air Force Awards Anchore Phase II Contract to Advance DevSecOps

The Air Force has awarded Anchore, a security solution provider, a phase II Small Business Innovation Research contract of $2.25 million. The award aims to boost DevSecOps-centered technology. A spokesperson for Anchore stated that they are excited to pioneer developments in the journey for wide-scale software application modernization across government | **(Read More)**

Pentagon Unveils New Defense Space Strategy

On June 17, the Pentagon unveiled a new Defense Space Strategy that aims to ensure the US maintains military superiority over advanced adversaries such as China and Russia. The new plan signifies the critical moment in space exploration that we are currently in. The US military is also increasingly shifting | **(Read More)**

OODA Loop Daily Pulse

This OODA Loop Daily brief is a hand-curated cyber and risk intelligence briefing covering the latest global threats and risk issues. For more information visit www.oodaloop.com

Copyright © 2020 OODA LLC, All rights reserved.
You subscribed to this list via our web site at www.ooda.com or www.oodaloop.com.

Our mailing address is:
OODA LLC
12110 Sunset Hills Road
Suite 600
RESTON, VA 20190

Add us to your address book

Want to change how you receive these emails?
You can **update your preferences** or **unsubscribe from this list**.

<!

The CyberWire 6.22.20: BlueLeaks dumps decades of police files. BlueKai data leaked. COVID-19 app privacy. Cyber conflict: China vs. India, Australia?

From: The CyberWire <editor@thecyberwire.com>

To: Keith.Morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: June 22, 2020 10:29:38 AM CDT

Received: June 22, 2020 10:29:52 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

More signal, less noise.

SPONSORED BY RECORDED FUTURE:

Get real-time security intelligence at no cost.

We recently launched Recorded Future Express — a free browser extension for security teams. Use Express over any web-based SIEM, vulnerability management solution, security blog, and more to put real-time security intelligence at your fingertips. Instantly prioritize alerts, incidents, and vulnerabilities based on real-time risk scores from the world's largest commercial collection platform. Sign up now.

Daily briefing.

June 22, 2020.

SUMMARY

By the CyberWire staff

Distributed Denial of Secrets (DDoSecrets), a hacktivist group described as an alternative to WikiLeaks, has posted BlueLeaks, "ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources. Among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more." The files are available, KrebsOnSecurityreports, in a searchable database. The National Fusion Center Association (NFCA) has confirmed the data's validity, saying the leaked files were compiled between August 1996 and June 19, 2020, which covers more than the decade DDoSecrets claimed in their tweeted communiqué. The breach appears to originate with a third party: NCFA believes the data were probably taken from Netsential (a contractor widely used by state fusion centers) by someone who gained entrance to the system using compromised user credentials.

TechCrunch reports that data collected on behalf of clients by Oracle's BlueKai, which uses cookies and "other tracking tech" to follow users as they browse the web, the better to develop profiles for marketing, were exposed in unsecured servers. Oracle believes the incident to be a misconfiguration issue on the part of two of its customers

The Washington Post summarizes two examinations of widely used COVID-19 contact-tracing and symptom-logging apps. Many are weakly encrypted, and several arguably overshare data with third parties.

India remains jittery over the prospect of Chinese cyberattacks, ET CIO reports. And judging from stories in the Australian Financial Review and elsewhere, Australia remains in high dudgeon over Chinese government hacking.

[250]

SPONSORED BY GDIT:

Secure your mission with the GDIT Cyber Stack, our ecosystem of cyber capabilities.

Notes.

Today's issue includes events affecting Australia, Canada, China, the European Union, France, India, Indonesia, Iran, Ireland, the Democratic People's Republic of Korea, the Republic of Korea, Morocco, the Netherlands, New Zealand, Pakistan, the Philippines, Russia, the United Kingdom, and the United States.

CSO Perspectives: Cyber Threat Intelligence, the fuel that drives the entire infosec engine.

By Rick Howard, CSO, Chief Analyst, and Senior Fellow, The CyberWire

Zero trust, intrusion kill chains, resilience, DevSecOps, and risk assessment are essential key strategies for preventing material impact to our organization due to a cyber event. The fuel

that drives that engine is cyber threat intelligence operations.

This week, we're talking about cyber threat intelligence in CyberWire Pro. Be sure to check out the essay and the accompanying podcast called Cybersecurity first principles: cyber threat intelligence operations on the CSO Perspectives section of the CyberWire Website.

SPONSORED BY MCAFEE:

Transition your enterprise to a secured, remote work environment with McAfee

Most companies aren't prepared to secure data and assets for a surge of remote employees. Whether your VPN is over capacity, new cloud services are coming on-board, or new devices need protection, we have you covered during this critical time. McAfee is offering 3-month subscriptions for Endpoint Protection, Unified Cloud Edge, and CASB to help you scale security to your remote employees. Learn more about these offers at mcafee.com/workfromhome.

ON THE PODCAST

In today's CyberWire Daily Podcast, out later this afternoon, we speak with Rick Howard, the CyberWire's CSO and Chief Analyst, who discusses intelligence operations and introduces Canon Week. Our inaugural Canon Week guest is Todd Fitzgerald, author of *CISO Compass*, a book about the challenges of cybersecurity leadership, with lessons learned from those who've met those challenges.

SPONSORED EVENTS

Cyber Security Summit Virtual Power Hours (Online, June 23 - 25, 2020) Senior Level Executives are invited to the Cyber Summit Virtual Power Hours. Learn from Industry Experts from The FBI, DHS, U.S. Secret Service & leading cyber solution providers as they discuss the latest security challenges & develop cyber security battle plans in today's unprecedented times. You will receive 1 CPE / CEU credit by attending. Free to register with code: CyberWire20 at CyberSummitUSA.com.

Improving Cyber-Oriented Education (Online, June 25, 2020) The Cyberspace Solarium Commission (CSC) recently released a report that proposes a strategy of layered cyber deterrence. Tune in to hear from CSC Commissioners and Industry leaders to discuss the report's findings, educational aspects, and opportunities to improve Cyber-oriented education.

FutureCon Virtual Eastern Conference (Online, June 30, 2020) This virtual event features thought-provoking presentations by Industry Security Leaders, esteemed Keynote Speakers, and a Panel Session discussion with experienced professionals and a talented team who are at the forefront of cutting edge strategies for Cybersecurity defense. 100% off promo code:

CYBERWIRE

IoT Integrator Summit: Securing Edge Computing (Online, July 14 - 16, 2020) A virtual summit to help IoT Integrators learn more about advances and updates in IoT security and discover new methods for architecting IoT solutions for your organization or your clients.

RSA Conference APJ July 15-17, 2020 - A Virtual Learning Experience (Online, July 15 - 17, 2020) The world's leading cybersecurity event is going virtual 15-17 July. Join your peers and industry experts for three days of insights. Watch over 50 sessions live during Singapore business hours—or stream them later. Register today for free.

SELECTED READING

Cyber Attacks, Threats, and Vulnerabilities

Journalist's phone hacked by new 'invisible' technique: All he had to do was visit one website. Any website. (Record) Moroccan journalist Omar Radi investigates connections between politicians and business people, as well...

NSO spyware used against Moroccan journalist days after company pledged to respect human rights (Amnesty International) NSO Group contributed to a sustained campaign by the government of Morocco to spy on Moroccan journalist...

Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools (Amnesty International) In October 2019 Amnesty International published a first report on the use of spyware produced by Israeli...

Find MORE on our website.

Cyber Trends

IBM Security Study Finds Employees New to Working from Home Pose Security Risk (IBM News Room) IBM (NYSE: IBM) Security today released findings from a study focused on the behaviors and security risks...

The Post-Pandemic Enterprise: What Will It Be Like? (Wall Street Journal) Enterprises should embrace and scale the changes, from supply chain optimization to remote work, they...

US Businesses Strengthen Their Cyber Defenses, but Blind Spots Remain, Reveals Annual Hiscox Cyber Readiness Report (PR Newswire) Hiscox, the international specialist insurer, revealed businesses are enhancing levels of spending and...

Find MORE on our website.

Marketplace

Microsoft Acquires IoT/OT Security Leader CyberX to Enable Unified Security Across Converged IT and Industrial Networks (Yahoo) Today, CyberX announced that it is being acquired by Microsoft.

With ransomware attacks increasing, cyber insurance now seen as a necessity, not a

luxury (Security Magazine) Threat actors launched a cyberattack against the Texas Office of Court Administration, the IT provider...

Air Force Space Accelerator Will Nurture Tech Startups Focused on Cybersecurity (Air Force Magazine) The Air Force Space Accelerator Program has opened the competition for its latest cohort of tech start-ups...

Find MORE on our website.

Products, Services, and Solutions

Centrifuge Addresses Growing IoT Compliance Standards (ReFirm Labs) The Spring 2020 release of the Centrifuge Platform introduces binary differencing and IoT security compliance...

Italy's Soft Strategy and ShadowDragon Partner to provide Investigative training and advanced investigative capabilities. (PR Newswire) Soft Strategy and ShadowDragon partner together to provide advanced investigative training. As the world...

Security Gaining Attention On IBM i, But More Progress Needed (IT Jungle) First, the good news: IBM i shops are paying more attention to security and are making it a priority,...

Find MORE on our website.

Technologies, Techniques, and Standards

NSA Updates Telework Tech Guide for Agencies (Meritalk) The National Security Agency (NSA) updated its telework tech security guidance June 4 with new details...

Does a generalization of tracking data cover up our traces on the internet? (Help Net Security) Computer scientists of KIT and TU Dresden study how well a generalization of tracking data covers up...

The UK's contact tracing app fiasco is a master class in mismanagement (MIT Technology Review) There are advantages to being one of the world's largest single-payer health-care systems. For the UK's...

Find MORE on our website.

Research and Development

CSIRO's Data61 develops voice detection technique to prevent voice spoofing attacks (ZDNet) Void can detect the 'liveness' of a voice.

Legislation, Policy, and Regulation

Commission reports on 2019 European elections: fostering European debates and securing free and fair elections (European Commission) Today, the European Commission has published its report on the conduct of the 2019 elections to the European...

Unification Ministry to Upgrade Computer System to Counter Cyberattacks from N. Korea (KBS World) South Korea's Unification Ministry will reportedly upgrade its computer

system to enhance security and...

China to establish 'national security agency' in Hong Kong (China to establish 'national security agency' in Hong Kong) The agency for semi-autonomous city will collect intelligence and handle crimes against national security,...

Find MORE on our website.

Litigation, Investigation, and Law Enforcement

China says espionage cases against Canadians not linked to Huawei CFO (WTVB) China said on Monday the espionage cases against two Canadian citizens in the country are unrelated to...

ACT govt urged to improve data security after shocker audit (iTnews) Agencies lacking understanding, awareness.

Wirecard Says Missing $2 Billion Probably Doesn't Exist (Wall Street Journal) The announcement leaves the company, once considered Germany's pre-eminent fintech player, fighting for...

Find MORE on our website.

INDUSTRY EVENTS

For a complete running list of events, please visit the Event Tracker on the CyberWire website.

Upcoming Events

WSIS Forum 2020 (, June 22 - September 10, 2020) The World Summit on the Information Society (WSIS) Forum 2020, celebrates 15 years of providing a multi-stakeholder...

Hardware Hacking Virtual Conference (Online, June 24, 2020) Join the ioXt Alliance and register now for our upcoming Summer Virtual Conference. You'll hear the latest...

Texas Cyber June'gle Virtual Summit (Online, June 27 - 28, 2020) The Texas Cyber June'gle Virtual Summit is June 27th and June 28th, it runs approximately 30 hours straight,...

FutureCon Virtual Eastern Conference (Online, June 30, 2020) This virtual event features thought-provoking presentations by Industry Security Leaders, esteemed Keynote...

CS4CA World: Global Cyber Security Event (Online, June 30, 2020) CS4CA World will take place virtually as a unique large-scale event to keep the critical asset community...

SPONSOR & SUPPORT

Grow your brand and reach new customers.

Grow your brand and increase your customer base by educating our audience about your products, services, and events by advertising on The CyberWire. We've built trust with an influential (and often hard to reach) audience of CISOs, CSOs, and other senior execs in the security space, across a wide array of industry verticals. Learn more.





Copyright © 2020, CyberWire Inc. Views and assertions of the various sources cited, Selected Reading articles, and cartoons are those of the authors and artists, not the CyberWire, Inc.

This email was sent to Keith.Morrison@cookcountyil.gov
why did I get this? | unsubscribe | update subscription preferences

The CyberWire · 8110 Maple Lawn Blvd. · Suite 200 · Fulton, Md 20759 · USA

IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Keith Morrison <Keith.Morrison@cookcountyil.gov>, Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Sent: June 23, 2020 6:09:30 AM CDT
Received: June 23, 2020 6:09:26 AM CDT

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

To:	Amar Patel (Sheriff), Keith Morrison, Adnan Memon (Sheriff)
Sent:	June 23, 2020 6:09:30 AM CDT
Received:	June 23, 2020 6:09:26 AM CDT

IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

To:	Amar Patel (Sheriff), Keith Morrison (Sheriff), Adnan Memon (Sheriff), isn@lists.infosecnews.org, Sheriff Intel, Jonathan Springborn (Sheriff), Christopher Moore (Sheriff), Patrick Kelly (Sheriff)
Sent:	June 23, 2020 6:09:46 AM CDT
Received:	June 23, 2020 6:09:48 AM CDT

IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

From:	Douglas Maclean (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=20EA5411E8A349589C43587009EDD10F-DOUGLAS MAC>
To:	Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>, Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Sent:	June 23, 2020 6:09:46 AM CDT
Received:	June 23, 2020 6:09:00 AM CDT

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

From:	Keith Morrison (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D2EBEC5431A14B10A53942341DBD54F4-KEITH MORRI>
To:	Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>, Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Sent:	June 23, 2020 6:19:51 AM CDT
Received:	June 23, 2020 6:19:00 AM CDT

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

FW: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
To: Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent: June 23, 2020 6:20:39 AM CDT
Received: June 23, 2020 6:20:40 AM CDT

No Action Needed

From: Keith Morrison (Sheriff)
Sent: Tuesday, June 23, 2020 6:20 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

FW: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

From: Keith Morrison (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D2EBEC5431A14B10A53942341DBD54F4-KEITH MORRI>
To: Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent: June 23, 2020 6:20:39 AM CDT
Received: June 23, 2020 6:20:00 AM CDT

No Action Needed

From: Keith Morrison (Sheriff)
Sent: Tuesday, June 23, 2020 6:20 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

FW: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

To:	Christopher Moore (Sheriff), Douglas Maclean (Sheriff), Amar Patel (Sheriff), Adnan Memon (Sheriff), Donna Fitzpatrick (Sheriff), Gregory.Wing@ic.fbi.gov, Michael.Tomasiello (Chicago Police), CCSO Intel (Sheriff), Kevin O'Donnell (Sheriff)
Cc:	Adnan Memon (Sheriff), Douglas Maclean (Sheriff), Amar Patel (Sheriff)
Sent:	June 23, 2020 6:20:39 AM CDT
Received:	June 23, 2020 6:20:00 AM CDT

RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

To:	Keith Morrison (Sheriff), Amar Patel (Sheriff), Adnan Memon (Sheriff), Patrick Kelly (Sheriff), Christopher Moore (Sheriff), Sheriff Intel, Jonathan Springborn (Sheriff), Michael Aliperti, Ben Spear
Cc:	Adnan Memon (Sheriff), Douglas Maclean (Sheriff)
Sent:	June 23, 2020 6:26:11 AM CDT
Received:	June 23, 2020 6:26:13 AM CDT

RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

From: Douglas Maclean (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=20EA5411E8A349589C43587009EDD10F-DOUGLAS MAC>
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>, Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Sent: June 23, 2020 6:26:11 AM CDT
Received: June 23, 2020 6:26:00 AM CDT

Keith –

[redacted]

Doug

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 6:20 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO

Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: jennifer.warren@cookcountyil.gov, Jennifer Warren (Sheriff) <jennifer.warren@cookcountyil.gov>

Sent: June 23, 2020 6:43:06 AM CDT
Received: June 23, 2020 6:43:21 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Jennifer Warren

Tuesday, June 23, 2020

POLICING & POLICY

US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police

ABC News (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday officially took a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforcement officers, despite intense national outcry over police misconduct and legal protections that shield cops from liability. 'The Supreme Court has made clear that they are not prepared to reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert on the doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 1871 gives Americans the unambiguous ability to sue public officials over civil rights violations, the Supreme Court subsequently limited liability to only those rights that have become 'clearly established law.'"

Newsday (NY) (6/22, Brune) reports that qualified immunity "shields police from being sued for money damages in federal court for constitutional violations such as excessive force unless the officers broke any 'clearly established' law – a high bar for plaintiffs to overcome." Newsday adds that police groups argue that ending qualified immunity "would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retirements and a smaller pool of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal standard will have a devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a statement."

Senate Democrats Threaten To Block GOP Police Reform Bill

Politico (6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week absent more concessions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester (D-MT) said, "If nothing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixing." Senate Minority Leader Schumer called the GOP bill "deeply and fundamentally flawed."

Reuters Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law. Reuters (6/22, Morgan) reports that the Senate and the House "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is expected to hold a procedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." However, Reuters says, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."

Studies Find Recreational Marijuana Laws May Boost Traffic Deaths

The AP (6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although questions remain about how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published Monday in JAMA Internal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an excess 75 traffic deaths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change in Washington state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalized recreational marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

Pandemic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

The New York Times (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the backlog of pending cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury trials in the city have been put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

Massachusetts Governor Seeks Training Bonuses For Police Officers

Boston (6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to $5,000 should they take on additional training under a bill filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize officers to go beyond the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law enforcement, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a system to uniformly certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first aid, de-escalation tactics, and narcotics training."

San Diego, California Ballot Measure Would Reform Police Oversight, Accountability

The San Diego Union-Tribune (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparency and accountability." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board with the power to launch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained momentum in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "completed negotiations May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by the commission that they are guilty of misconduct."

Join the IACP on June 24, 2020, at 1:00 p.m. EST for Part 2 and July 16, 2020, at 1:00 p.m. EST for Part 3 of *Mindfulness Strategies for Law Enforcement* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety Initiatives Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim services personnel, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute interactive mindfulness sessions.

Reserve you space.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Swedish Rape Conviction Rates Rise 75% After Change In Law

Reuters (6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls on Monday for other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. Unlike in many countries, prosecutors do not have to prove the use or threat of violence or coercion. The National Council on Crime Prevention (Bra) said the rise in convictions – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected." According to Reuters, "Britain, Belgium, Canada, Cyprus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Portugal have promised similar reforms."

New York City Raid Leads To Drug Seizures, Two Arrests

The New York Post (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of "approximately 1.2 kilograms of heroin, 34 grams of fentanyl and 2.3 kilograms of methamphetamine." Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who face "charges of criminal possession of a controlled substance and criminally using drug paraphernalia." The arrests were the result of joint operation conducted by "the city's Special Narcotics Prosecutor," the City of New York Police Department, and the DEA.

UK Drinkers Barricade Themselves In Pub During Illegal Lockdown Lock-In

The Independent (UK) (6/22, Gregory) reports, "Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police officers arrived to break up the session, according to police." According to the Independent, "Merseyside Police officers were pelted with beer and other items as revellers took up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered at the Vauxhall pub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only 'a number of people' were said to take part in the blockade." The Independent adds, "Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs have been closed by law for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a range of new measures in place to protect customers."

TECHNOLOGY

"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers

The Blaze (6/22, Taylor) reports hackers have "leaked highly sensitive police files from over 200 police departments across the country." Activist group DDoSecrets "published what the outlet calls 'hundreds of gigabytes' worth of potentially sensitive files' from police departments across the US." The group has "called the information dump 'BlueLeaks.'" The group "compiled the records, disseminating them into a searchable database that can pull up private information from a police badge number." Many of the files include "information such as memos, emails, and officers' personal information". The group "shared information on Twitter regarding the data dump."

GLOBAL SECURITY

NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally

The New York Times (6/22, Alba, Decker) examines how in recent weeks, "residents in at least 41 U.S. cities and towns became alarmed by rumors that the loose collective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, they contacted their local law enforcement for help. In each case, it was for a threat that never appeared." On the local level, the analysis found that "the source of the false information has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appears in a Twitter or Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking app Nextdoor and community texting networks," which "can fall under the radar of the tech companies and online fact checkers."

Black Lives Matter Protests Spread To White, Rural Areas. The Wall Street Journal (6/22, Carlton, Subscription Publication) reports that the protests for racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

MONDAY'S LEAD STORIES

- **Former IACP President Addresses Police Reform**
- **UK Authorities Grapple With Illegal "Quarantine Raves"**
- **Libyan Refugee Arrested In UK Terrorist Attack That Left Three Dead**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to jennifer.warren@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: brian.white@cookcountyil.gov, Brian White (Sheriff) <Brian.White@cookcountyil.gov>

Sent: June 23, 2020 6:43:06 AM CDT
Received: June 23, 2020 6:43:17 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Brian White

Tuesday, June 23, 2020

POLICING & POLICY

US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police

ABC News (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday officially took a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforcement officers, despite intense national outcry over police misconduct and legal protections that shield cops from liability. 'The Supreme Court has made clear that they are not prepared to reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert on the doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 1871 gives Americans the unambiguous ability to sue public officials over civil rights violations, the Supreme Court subsequently limited liability to only those rights that have become 'clearly established law.'"

Newsday (NY) (6/22, Brune) reports that qualified immunity "shields police from being sued for money damages in federal court for constitutional violations such as excessive force unless the officers broke any 'clearly established' law – a high bar for plaintiffs to overcome." Newsday adds that police groups argue that ending qualified immunity "would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retirements and a smaller pool of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal standard will have a devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a statement."

Senate Democrats Threaten To Block GOP Police Reform Bill

Politico (6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week absent more concessions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester (D-MT) said, "If nothing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixing." Senate Minority Leader Schumer called the GOP bill "deeply and fundamentally flawed."

Reuters Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law. Reuters (6/22, Morgan) reports that the Senate and the House "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is expected to hold a procedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." However, Reuters says, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."

Studies Find Recreational Marijuana Laws May Boost Traffic Deaths

The AP (6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although questions remain about how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published Monday in JAMA Internal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an excess 75 traffic deaths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change in Washington state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalized recreational marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

Pandemic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

The New York Times (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the backlog of pending cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury trials in the city have been put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

Massachusetts Governor Seeks Training Bonuses For Police Officers

Boston (6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to $5,000 should they take on additional training under a bill filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize officers to go beyond the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law enforcement, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a system to uniformly certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first aid, de-escalation tactics, and narcotics training."

San Diego, California Ballot Measure Would Reform Police Oversight, Accountability

The San Diego Union-Tribune (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparency and accountability." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board with the power to launch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained momentum in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "completed negotiations May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by the commission that they are guilty of misconduct."

Join the IACP on June 24, 2020, at 1:00 p.m. EST for Part 2 and July 16, 2020, at 1:00 p.m. EST for Part 3 of *Mindfulness Strategies for Law Enforcement* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety Initiatives Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim services personnel, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute interactive mindfulness sessions.

Reserve you space.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Swedish Rape Conviction Rates Rise 75% After Change In Law

Reuters (6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls on Monday for other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. Unlike in many countries, prosecutors do not have to prove the use or threat of violence or coercion. The National Council on Crime Prevention (Bra) said the rise in convictions – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected." According to Reuters, "Britain, Belgium, Canada, Cyprus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Portugal have promised similar reforms."

New York City Raid Leads To Drug Seizures, Two Arrests

The New York Post (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of "approximately 1.2 kilograms of heroin, 34 grams of fentanyl and 2.3 kilograms of methamphetamine." Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who face "charges of criminal possession of a controlled substance and criminally using drug paraphernalia." The arrests were the result of joint operation conducted by "the city's Special Narcotics Prosecutor," the City of New York Police Department, and the DEA.

UK Drinkers Barricade Themselves In Pub During Illegal Lockdown Lock-In

The Independent (UK) (6/22, Gregory) reports, "Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police officers arrived to break up the session, according to police." According to the Independent, "Merseyside Police officers were pelted with beer and other items as revellers took up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered at the Vauxhall pub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only 'a number of people' were said to take part in the blockade." The Independent adds, "Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs have been closed by law for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a range of new measures in place to protect customers."

TECHNOLOGY

"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers

The Blaze (6/22, Taylor) reports hackers have "leaked highly sensitive police files from over 200 police departments across the country." Activist group DDoSecrets "published what the outlet calls 'hundreds of gigabytes' worth of potentially sensitive files' from police departments across the US." The group has "called the information dump 'BlueLeaks.'" The group "compiled the records, disseminating them into a searchable database that can pull up private information from a police badge number." Many of the files include "information such as memos, emails, and officers' personal information". The group "shared information on Twitter regarding the data dump."

GLOBAL SECURITY

NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally

The New York Times (6/22, Alba, Decker) examines how in recent weeks, "residents in at least 41 U.S. cities and towns became alarmed by rumors that the loose collective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, they contacted their local law enforcement for help. In each case, it was for a threat that never appeared." On the local level, the analysis found that "the source of the false information has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appears in a Twitter or Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking app Nextdoor and community texting networks," which "can fall under the radar of the tech companies and online fact checkers."

Black Lives Matter Protests Spread To White, Rural Areas. The Wall Street Journal (6/22, Carlton, Subscription Publication) reports that the protests for racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

MONDAY'S LEAD STORIES

- **Former IACP President Addresses Police Reform**
- **UK Authorities Grapple With Illegal "Quarantine Raves"**
- **Libyan Refugee Arrested In UK Terrorist Attack That Left Three Dead**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to brian.white@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: keith.morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: June 23, 2020 6:43:06 AM CDT
Received: June 23, 2020 6:43:21 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Keith Morrison Tuesday, June 23, 2020

POLICING & POLICY

US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police

ABC News (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday officially took a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforcement officers, despite intense national outcry over police misconduct and legal protections that shield cops from liability. 'The Supreme Court has made clear that they are not prepared to reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert on the doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 1871 gives Americans the unambiguous ability to sue public officials over civil rights violations, the Supreme Court subsequently limited liability to only those rights that have become 'clearly established law.'"

Newsday (NY) (6/22, Brune) reports that qualified immunity "shields police from being sued for money damages in federal court for constitutional violations such as excessive force unless the officers broke any 'clearly established' law – a high bar for plaintiffs to overcome." Newsday adds that police groups argue that ending qualified immunity "would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retirements and a smaller pool of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal standard will have a devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a statement."

Senate Democrats Threaten To Block GOP Police Reform Bill

Politico (6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week absent more concessions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester (D-MT) said, "If nothing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixing." Senate Minority Leader Schumer called the GOP bill "deeply and fundamentally flawed."

Reuters Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law. Reuters (6/22, Morgan) reports that the Senate and the House "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is expected to hold a procedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." However, Reuters says, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."

Studies Find Recreational Marijuana Laws May Boost Traffic Deaths

The AP (6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although questions remain about how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published Monday in JAMA Internal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an excess 75 traffic deaths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change in Washington state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalized recreational marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

Pandemic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

The New York Times (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the backlog of pending cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury trials in the city have been put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

Massachusetts Governor Seeks Training Bonuses For Police Officers

Boston (6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to $5,000 should they take on additional training under a bill filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize officers to go beyond the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law enforcement, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a system to uniformly certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first aid, de-escalation tactics, and narcotics training."

San Diego, California Ballot Measure Would Reform Police Oversight, Accountability

The San Diego Union-Tribune (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparency and accountability." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board with the power to launch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained momentum in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "completed negotiations May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by the commission that they are guilty of misconduct."

Join the IACP on June 24, 2020, at 1:00 p.m. EST for Part 2 and July 16, 2020, at 1:00 p.m. EST for Part 3 of *Mindfulness Strategies for Law Enforcement* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety Initiatives Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim services personnel, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute interactive mindfulness sessions.

Reserve you space.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Swedish Rape Conviction Rates Rise 75% After Change In Law

Reuters (6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls on Monday for other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. Unlike in many countries, prosecutors do not have to prove the use or threat of violence or coercion. The National Council on Crime Prevention (Bra) said the rise in convictions – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected." According to Reuters, "Britain, Belgium, Canada, Cyprus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Portugal have promised similar reforms."

New York City Raid Leads To Drug Seizures, Two Arrests

The New York Post (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of "approximately 1.2 kilograms of heroin, 34 grams of fentanyl and 2.3 kilograms of methamphetamine." Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who face "charges of criminal possession of a controlled substance and criminally using drug paraphernalia." The arrests were the result of joint operation conducted by "the city's Special Narcotics Prosecutor," the City of New York Police Department, and the DEA.

UK Drinkers Barricade Themselves In Pub During Illegal Lockdown Lock-In

The Independent (UK) (6/22, Gregory) reports, "Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police officers arrived to break up the session, according to police." According to the Independent, "Merseyside Police officers were pelted with beer and other items as revellers took up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered at the Vauxhall pub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only 'a number of people' were said to take part in the blockade." The Independent adds, "Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs have been closed by law for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a range of new measures in place to protect customers."

TECHNOLOGY

"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers

The Blaze (6/22, Taylor) reports hackers have "leaked highly sensitive police files from over 200 police departments across the country." Activist group DDoSecrets "published what the outlet calls 'hundreds of gigabytes' worth of potentially sensitive files' from police departments across the US." The group has "called the information dump 'BlueLeaks.'" The group "compiled the records, disseminating them into a searchable database that can pull up private information from a police badge number." Many of the files include "information such as memos, emails, and officers' personal information". The group "shared information on Twitter regarding the data dump."

GLOBAL SECURITY

NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally

The New York Times (6/22, Alba, Decker) examines how in recent weeks, "residents in at least 41 U.S. cities and towns became alarmed by rumors that the loose collective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, they contacted their local law enforcement for help. In each case, it was for a threat that never appeared." On the local level, the analysis found that "the source of the false information has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appears in a Twitter or Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking app Nextdoor and community texting networks," which "can fall under the radar of the tech companies and online fact checkers."

Black Lives Matter Protests Spread To White, Rural Areas. The Wall Street Journal (6/22, Carlton, Subscription Publication) reports that the protests for racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

MONDAY'S LEAD STORIES

- **Former IACP President Addresses Police Reform**
- **UK Authorities Grapple With Illegal "Quarantine Raves"**
- **Libyan Refugee Arrested In UK Terrorist Attack That Left Three Dead**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to keith.morrison@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: sean.gleason@cookcountyil.gov, Sean Gleason (Sheriff) <Sean.Gleason@cookcountyil.gov>

Sent: June 23, 2020 6:43:06 AM CDT
Received: June 23, 2020 6:43:10 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Sean Gleason

Tuesday, June 23, 2020

POLICING & POLICY

US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police

ABC News (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday officially took a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforcement officers, despite intense national outcry over police misconduct and legal protections that shield cops from liability. 'The Supreme Court has made clear that they are not prepared to reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert on the doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 1871 gives Americans the unambiguous ability to sue public officials over civil rights violations, the Supreme Court subsequently limited liability to only those rights that have become 'clearly established law.'"

Newsday (NY) (6/22, Brune) reports that qualified immunity "shields police from being sued for money damages in federal court for constitutional violations such as excessive force unless the officers broke any 'clearly established' law – a high bar for plaintiffs to overcome." Newsday adds that police groups argue that ending qualified immunity "would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retirements and a smaller pool of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal standard will have a devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a statement."

Senate Democrats Threaten To Block GOP Police Reform Bill

Politico (6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week absent more concessions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester (D-MT) said, "If nothing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixing." Senate Minority Leader Schumer called the GOP bill "deeply and fundamentally flawed."

Reuters Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law. Reuters (6/22, Morgan) reports that the Senate and the House "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is expected to hold a procedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." However, Reuters says, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."

Studies Find Recreational Marijuana Laws May Boost Traffic Deaths

The AP (6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although questions remain about how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published Monday in JAMA Internal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an excess 75 traffic deaths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change in Washington state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalized recreational marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

Pandemic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

The New York Times (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the backlog of pending cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury trials in the city have been put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

Massachusetts Governor Seeks Training Bonuses For Police Officers

Boston (6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to $5,000 should they take on additional training under a bill filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize officers to go beyond the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law enforcement, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a system to uniformly certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first aid, de-escalation tactics, and narcotics training."

San Diego, California Ballot Measure Would Reform Police Oversight, Accountability

The San Diego Union-Tribune (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparency and accountability." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board with the power to launch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained momentum in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "completed negotiations May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by the commission that they are guilty of misconduct."

Join the IACP on June 24, 2020, at 1:00 p.m. EST for Part 2 and July 16, 2020, at 1:00 p.m. EST for Part 3 of *Mindfulness Strategies for Law Enforcement* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety Initiatives Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim services personnel, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute interactive mindfulness sessions.

Reserve you space.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Swedish Rape Conviction Rates Rise 75% After Change In Law

Reuters (6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls on Monday for other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. Unlike in many countries, prosecutors do not have to prove the use or threat of violence or coercion. The National Council on Crime Prevention (Bra) said the rise in convictions – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected." According to Reuters, "Britain, Belgium, Canada, Cyprus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Portugal have promised similar reforms."

New York City Raid Leads To Drug Seizures, Two Arrests

The New York Post (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of "approximately 1.2 kilograms of heroin, 34 grams of fentanyl and 2.3 kilograms of methamphetamine." Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who face "charges of criminal possession of a controlled substance and criminally using drug paraphernalia." The arrests were the result of joint operation conducted by "the city's Special Narcotics Prosecutor," the City of New York Police Department, and the DEA.

UK Drinkers Barricade Themselves In Pub During Illegal Lockdown Lock-In

The Independent (UK) (6/22, Gregory) reports, "Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police officers arrived to break up the session, according to police." According to the Independent, "Merseyside Police officers were pelted with beer and other items as revellers took up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered at the Vauxhall pub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only 'a number of people' were said to take part in the blockade." The Independent adds, "Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs have been closed by law for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a range of new measures in place to protect customers."

TECHNOLOGY

"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers

The Blaze (6/22, Taylor) reports hackers have "leaked highly sensitive police files from over 200 police departments across the country." Activist group DDoSecrets "published what the outlet calls 'hundreds of gigabytes' worth of potentially sensitive files' from police departments across the US." The group has "called the information dump 'BlueLeaks.'" The group "compiled the records, disseminating them into a searchable database that can pull up private information from a police badge number." Many of the files include "information such as memos, emails, and officers' personal information". The group "shared information on Twitter regarding the data dump."

GLOBAL SECURITY

NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally

The New York Times (6/22, Alba, Decker) examines how in recent weeks, "residents in at least 41 U.S. cities and towns became alarmed by rumors that the loose collective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, they contacted their local law enforcement for help. In each case, it was for a threat that never appeared." On the local level, the analysis found that "the source of the false information has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appears in a Twitter or Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking app Nextdoor and community texting networks," which "can fall under the radar of the tech companies and online fact checkers."

Black Lives Matter Protests Spread To White, Rural Areas. The Wall Street Journal (6/22, Carlton, Subscription Publication) reports that the protests for racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

MONDAY'S LEAD STORIES

- **Former IACP President Addresses Police Reform**
- **UK Authorities Grapple With Illegal "Quarantine Raves"**
- **Libyan Refugee Arrested In UK Terrorist Attack That Left Three Dead**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to sean.gleason@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: noureen.kapadia@cookcountyil.gov, Noureen Kapadia (Sheriff) <Noureen.Kapadia@cookcountyil.gov>

Sent: June 23, 2020 6:43:06 AM CDT
Received: June 23, 2020 6:43:22 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Noureen Kapadia Tuesday, June 23, 2020

POLICING & POLICY

US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police

ABC News (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday officially took a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforcement officers, despite intense national outcry over police misconduct and legal protections that shield cops from liability. 'The Supreme Court has made clear that they are not prepared to reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert on the doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 1871 gives Americans the unambiguous ability to sue public officials over civil rights violations, the Supreme Court subsequently limited liability to only those rights that have become 'clearly established law.'"

Newsday (NY) (6/22, Brune) reports that qualified immunity "shields police from being sued for money damages in federal court for constitutional violations such as excessive force unless the officers broke any 'clearly established' law – a high bar for plaintiffs to overcome." Newsday adds that police groups argue that ending qualified immunity "would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retirements and a smaller pool of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal standard will have a devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a statement."

Senate Democrats Threaten To Block GOP Police Reform Bill

Politico (6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week absent more concessions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester (D-MT) said, "If nothing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixing." Senate Minority Leader Schumer called the GOP bill "deeply and fundamentally flawed."

Reuters Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law. Reuters (6/22, Morgan) reports that the Senate and the House "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is expected to hold a procedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." However, Reuters says, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."

Studies Find Recreational Marijuana Laws May Boost Traffic Deaths

The AP (6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although questions remain about how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published Monday in JAMA Internal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an excess 75 traffic deaths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change in Washington state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalized recreational marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

Pandemic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

The New York Times (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the backlog of pending cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury trials in the city have been put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

Massachusetts Governor Seeks Training Bonuses For Police Officers

Boston (6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to $5,000 should they take on additional training under a bill filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize officers to go beyond the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law enforcement, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a system to uniformly certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first aid, de-escalation tactics, and narcotics training."

San Diego, California Ballot Measure Would Reform Police Oversight, Accountability

The San Diego Union-Tribune (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparency and accountability." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board with the power to launch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained momentum in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "completed negotiations May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by the commission that they are guilty of misconduct."

Join the IACP on June 24, 2020, at 1:00 p.m. EST for Part 2 and July 16, 2020, at 1:00 p.m. EST for Part 3 of *Mindfulness Strategies for Law Enforcement* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety Initiatives Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim services personnel, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute interactive mindfulness sessions.

Reserve you space.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Swedish Rape Conviction Rates Rise 75% After Change In Law

Reuters (6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls on Monday for other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. Unlike in many countries, prosecutors do not have to prove the use or threat of violence or coercion. The National Council on Crime Prevention (Bra) said the rise in convictions – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected." According to Reuters, "Britain, Belgium, Canada, Cyprus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Portugal have promised similar reforms."

New York City Raid Leads To Drug Seizures, Two Arrests

The New York Post (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of "approximately 1.2 kilograms of heroin, 34 grams of fentanyl and 2.3 kilograms of methamphetamine." Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who face "charges of criminal possession of a controlled substance and criminally using drug paraphernalia." The arrests were the result of joint operation conducted by "the city's Special Narcotics Prosecutor," the City of New York Police Department, and the DEA.

UK Drinkers Barricade Themselves In Pub During Illegal Lockdown Lock-In

The Independent (UK) (6/22, Gregory) reports, "Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police officers arrived to break up the session, according to police." According to the Independent, "Merseyside Police officers were pelted with beer and other items as revellers took up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered at the Vauxhall pub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only 'a number of people' were said to take part in the blockade." The Independent adds, "Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs have been closed by law for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a range of new measures in place to protect customers."

TECHNOLOGY

"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers

The Blaze (6/22, Taylor) reports hackers have "leaked highly sensitive police files from over 200 police departments across the country." Activist group DDoSecrets "published what the outlet calls 'hundreds of gigabytes' worth of potentially sensitive files' from police departments across the US." The group has "called the information dump 'BlueLeaks.'" The group "compiled the records, disseminating them into a searchable database that can pull up private information from a police badge number." Many of the files include "information such as memos, emails, and officers' personal information". The group "shared information on Twitter regarding the data dump."

GLOBAL SECURITY

NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally

The New York Times (6/22, Alba, Decker) examines how in recent weeks, "residents in at least 41 U.S. cities and towns became alarmed by rumors that the loose collective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, they contacted their local law enforcement for help. In each case, it was for a threat that never appeared." On the local level, the analysis found that "the source of the false information has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appears in a Twitter or Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking app Nextdoor and community texting networks," which "can fall under the radar of the tech companies and online fact checkers."

Black Lives Matter Protests Spread To White, Rural Areas. The Wall Street Journal (6/22, Carlton, Subscription Publication) reports that the protests for racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

MONDAY'S LEAD STORIES

- **Former IACP President Addresses Police Reform**
- **UK Authorities Grapple With Illegal "Quarantine Raves"**
- **Libyan Refugee Arrested In UK Terrorist Attack That Left Three Dead**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to noureen.kapadia@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: thomas.conley@cookcountyil.gov, Thomas Conley (Sheriff) <Thomas.Conley@cookcountyil.gov>

Sent: June 23, 2020 6:43:06 AM CDT
Received: June 23, 2020 6:43:21 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Thomas Conley

Tuesday, June 23, 2020

POLICING & POLICY

US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police

ABC News (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday officially took a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforcement officers, despite intense national outcry over police misconduct and legal protections that shield cops from liability. 'The Supreme Court has made clear that they are not prepared to reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert on the doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 1871 gives Americans the unambiguous ability to sue public officials over civil rights violations, the Supreme Court subsequently limited liability to only those rights that have become 'clearly established law.'"

Newsday (NY) (6/22, Brune) reports that qualified immunity "shields police from being sued for money damages in federal court for constitutional violations such as excessive force unless the officers broke any 'clearly established' law – a high bar for plaintiffs to overcome." Newsday adds that police groups argue that ending qualified immunity "would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retirements and a smaller pool of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal standard will have a devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a statement."

Senate Democrats Threaten To Block GOP Police Reform Bill

Politico (6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week absent more concessions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester (D-MT) said, "If nothing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixing." Senate Minority Leader Schumer called the GOP bill "deeply and fundamentally flawed."

Reuters Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law. Reuters (6/22, Morgan) reports that the Senate and the House "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is expected to hold a procedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." However, Reuters says, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."

Studies Find Recreational Marijuana Laws May Boost Traffic Deaths

The AP (6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although questions remain about how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published Monday in JAMA Internal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an excess 75 traffic deaths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change in Washington state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalized recreational marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

Pandemic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

The New York Times (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the backlog of pending cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury trials in the city have been put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

Massachusetts Governor Seeks Training Bonuses For Police Officers

Boston (6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to $5,000 should they take on additional training under a bill filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize officers to go beyond the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law enforcement, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a system to uniformly certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first aid, de-escalation tactics, and narcotics training."

San Diego, California Ballot Measure Would Reform Police Oversight, Accountability

The San Diego Union-Tribune (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparency and accountability." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board with the power to launch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained momentum in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "completed negotiations May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by the commission that they are guilty of misconduct."

Join the IACP on June 24, 2020, at 1:00 p.m. EST for Part 2 and July 16, 2020, at 1:00 p.m. EST for Part 3 of *Mindfulness Strategies for Law Enforcement* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety Initiatives Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim services personnel, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute interactive mindfulness sessions.

Reserve you space.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Swedish Rape Conviction Rates Rise 75% After Change In Law

Reuters (6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls on Monday for other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. Unlike in many countries, prosecutors do not have to prove the use or threat of violence or coercion. The National Council on Crime Prevention (Bra) said the rise in convictions – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected." According to Reuters, "Britain, Belgium, Canada, Cyprus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Portugal have promised similar reforms."

New York City Raid Leads To Drug Seizures, Two Arrests

The New York Post (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of "approximately 1.2 kilograms of heroin, 34 grams of fentanyl and 2.3 kilograms of methamphetamine." Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who face "charges of criminal possession of a controlled substance and criminally using drug paraphernalia." The arrests were the result of joint operation conducted by "the city's Special Narcotics Prosecutor," the City of New York Police Department, and the DEA.

UK Drinkers Barricade Themselves In Pub During Illegal Lockdown Lock-In

The Independent (UK) (6/22, Gregory) reports, "Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police officers arrived to break up the session, according to police." According to the Independent, "Merseyside Police officers were pelted with beer and other items as revellers took up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered at the Vauxhall pub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only 'a number of people' were said to take part in the blockade." The Independent adds, "Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs have been closed by law for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a range of new measures in place to protect customers."

TECHNOLOGY

"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers

The Blaze (6/22, Taylor) reports hackers have "leaked highly sensitive police files from over 200 police departments across the country." Activist group DDoSecrets "published what the outlet calls 'hundreds of gigabytes' worth of potentially sensitive files' from police departments across the US." The group has "called the information dump 'BlueLeaks.'" The group "compiled the records, disseminating them into a searchable database that can pull up private information from a police badge number." Many of the files include "information such as memos, emails, and officers' personal information". The group "shared information on Twitter regarding the data dump."

GLOBAL SECURITY

NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally

The New York Times (6/22, Alba, Decker) examines how in recent weeks, "residents in at least 41 U.S. cities and towns became alarmed by rumors that the loose collective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, they contacted their local law enforcement for help. In each case, it was for a threat that never appeared." On the local level, the analysis found that "the source of the false information has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appears in a Twitter or Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking app Nextdoor and community texting networks," which "can fall under the radar of the tech companies and online fact checkers."

Black Lives Matter Protests Spread To White, Rural Areas. The Wall Street Journal (6/22, Carlton, Subscription Publication) reports that the protests for racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

MONDAY'S LEAD STORIES

- **Former IACP President Addresses Police Reform**
- **UK Authorities Grapple With Illegal "Quarantine Raves"**
- **Libyan Refugee Arrested In UK Terrorist Attack That Left Three Dead**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to thomas.conley@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: theresa.olson@cookcountyil.gov, Theresa Olson (Sheriff) <Theresa.Olson@cookcountyil.gov>

Sent: June 23, 2020 6:43:06 AM CDT
Received: June 23, 2020 6:43:18 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Theresa Olson

Tuesday, June 23, 2020

POLICING & POLICY

US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police

ABC News (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday officially took a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforcement officers, despite intense national outcry over police misconduct and legal protections that shield cops from liability. 'The Supreme Court has made clear that they are not prepared to reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert on the doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 1871 gives Americans the unambiguous ability to sue public officials over civil rights violations, the Supreme Court subsequently limited liability to only those rights that have become 'clearly established law.'"

Newsday (NY) (6/22, Brune) reports that qualified immunity "shields police from being sued for money damages in federal court for constitutional violations such as excessive force unless the officers broke any 'clearly established' law – a high bar for plaintiffs to overcome." Newsday adds that police groups argue that ending qualified immunity "would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retirements and a smaller pool of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal standard will have a devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a statement."

Senate Democrats Threaten To Block GOP Police Reform Bill

Politico (6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week absent more concessions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester (D-MT) said, "If nothing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixing." Senate Minority Leader Schumer called the GOP bill "deeply and fundamentally flawed."

Reuters Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law. Reuters (6/22, Morgan) reports that the Senate and the House "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is expected to hold a procedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." However, Reuters says, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."

Studies Find Recreational Marijuana Laws May Boost Traffic Deaths

The AP (6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although questions remain about how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published Monday in JAMA Internal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an excess 75 traffic deaths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change in Washington state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalized recreational marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

Pandemic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

The New York Times (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the backlog of pending cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury trials in the city have been put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

Massachusetts Governor Seeks Training Bonuses For Police Officers

Boston (6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to $5,000 should they take on additional training under a bill filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize officers to go beyond the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law enforcement, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a system to uniformly certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first aid, de-escalation tactics, and narcotics training."

San Diego, California Ballot Measure Would Reform Police Oversight, Accountability

The San Diego Union-Tribune (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparency and accountability." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board with the power to launch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained momentum in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "completed negotiations May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by the commission that they are guilty of misconduct."

Join the IACP on June 24, 2020, at 1:00 p.m. EST for Part 2 and July 16, 2020, at 1:00 p.m. EST for Part 3 of *Mindfulness Strategies for Law Enforcement* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety Initiatives Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim services personnel, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute interactive mindfulness sessions.

Reserve you space.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Swedish Rape Conviction Rates Rise 75% After Change In Law

Reuters (6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls on Monday for other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. Unlike in many countries, prosecutors do not have to prove the use or threat of violence or coercion. The National Council on Crime Prevention (Bra) said the rise in convictions – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected." According to Reuters, "Britain, Belgium, Canada, Cyprus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Portugal have promised similar reforms."

New York City Raid Leads To Drug Seizures, Two Arrests

The New York Post (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of "approximately 1.2 kilograms of heroin, 34 grams of fentanyl and 2.3 kilograms of methamphetamine." Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who face "charges of criminal possession of a controlled substance and criminally using drug paraphernalia." The arrests were the result of joint operation conducted by "the city's Special Narcotics Prosecutor," the City of New York Police Department, and the DEA.

UK Drinkers Barricade Themselves In Pub During Illegal Lockdown Lock-In

The Independent (UK) (6/22, Gregory) reports, "Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police officers arrived to break up the session, according to police." According to the Independent, "Merseyside Police officers were pelted with beer and other items as revellers took up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered at the Vauxhall pub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only 'a number of people' were said to take part in the blockade." The Independent adds, "Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs have been closed by law for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a range of new measures in place to protect customers."

TECHNOLOGY

"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers

The Blaze (6/22, Taylor) reports hackers have "leaked highly sensitive police files from over 200 police departments across the country." Activist group DDoSecrets "published what the outlet calls 'hundreds of gigabytes' worth of potentially sensitive files' from police departments across the US." The group has "called the information dump 'BlueLeaks.'" The group "compiled the records, disseminating them into a searchable database that can pull up private information from a police badge number." Many of the files include "information such as memos, emails, and officers' personal information". The group "shared information on Twitter regarding the data dump."

GLOBAL SECURITY

NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally

The New York Times (6/22, Alba, Decker) examines how in recent weeks, "residents in at least 41 U.S. cities and towns became alarmed by rumors that the loose collective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, they contacted their local law enforcement for help. In each case, it was for a threat that never appeared." On the local level, the analysis found that "the source of the false information has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appears in a Twitter or Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking app Nextdoor and community texting networks," which "can fall under the radar of the tech companies and online fact checkers."

Black Lives Matter Protests Spread To White, Rural Areas. The Wall Street Journal (6/22, Carlton, Subscription Publication) reports that the protests for racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

MONDAY'S LEAD STORIES

- **Former IACP President Addresses Police Reform**
- **UK Authorities Grapple With Illegal "Quarantine Raves"**
- **Libyan Refugee Arrested In UK Terrorist Attack That Left Three Dead**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to theresa.olson@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Sent: June 23, 2020 6:44:57 AM CDT
Received: June 23, 2020 6:44:53 AM CDT

1. [redacted]

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:26 AM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Keith –

[redacted]

Doug

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 6:20 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

From:	Keith Morrison (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D2EBEC5431A14B10A53942341DBD54F4-KEITH MORRI>
To:	Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Sent:	June 23, 2020 6:45:11 AM CDT
Received:	June 23, 2020 6:45:00 AM CDT

[redacted]

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:26 AM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Keith –

[redacted]

Doug

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 6:20 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

FW: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
To: Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent: June 23, 2020 6:45:25 AM CDT
Received: June 23, 2020 6:45:25 AM CDT

From: Keith Morrison (Sheriff)
Sent: Tuesday, June 23, 2020 6:45 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

[redacted]

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:26 AM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Keith –

[redacted]

Doug

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 6:20 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

FW: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

From: Keith Morrison (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D2EBEC5431A14B10A53942341DBD54F4-KEITH MORRI>
To: Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent: June 23, 2020 6:45:25 AM CDT
Received: June 23, 2020 6:45:00 AM CDT

From: Keith Morrison (Sheriff)
Sent: Tuesday, June 23, 2020 6:45 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

[redacted]

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:26 AM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Keith –

[redacted]

Doug

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 6:20 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

FW: IACP's The Lead: Massachusetts Governor Seeks Training Bonuses For Police Officers

From:	Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
To:	Kevin O'Donnell (Sheriff) <Kevin.Odonnell@cookcountyil.gov>
Sent:	June 23, 2020 6:52:01 AM CDT
Received:	June 23, 2020 6:52:02 AM CDT

From: The IACP [mailto:TheLead@iacp.bulletinmedia.com]
Sent: Tuesday, June 23, 2020 6:43 AM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Subject: IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

ith Morrison Tuesday, J

POLICING & POLICY

US Supreme Court Will Not Revisit Challenge To Qualified Immu Police

ABC News (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday off a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforc officers, despite intense national outcry over police misconduct and legal protect shield cops from liability. 'The Supreme Court has made clear that they are not pr reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert o doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 18 Americans the unambiguous ability to sue public officials over civil rights violation Supreme Court subsequently limited liability to only those rights that have becon established law.'"

Newsday (NY) (6/22, Brune) reports that qualified immunity "shields p from being sued for money damages in federal court for constitutional violations excessive force unless the officers broke any 'clearly established' law – a high bar plaintiffs to overcome." Newsday adds that police groups argue that ending quali 'would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retiremen ol of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a stateme

Democrats Threaten To Block GOP Police Reform Bill

(6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week essions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester thing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixin eader Schumer called the GOP bill "deeply and fundamentally flawed."

rs Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law. Reuters (6/22, Morgan) reports that the Sen "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is e cedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." How ys, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."

Find Recreational Marijuana Laws May Boost Traffic Deaths

(6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although quest out how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published rnal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an exc ths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change n state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalize al marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

ic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

ork Times (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury t een put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

usetts Governor Seeks Training Bonuses For Police Officers

(6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to $5,000 should they take on additional tr l filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize o the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law nt, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a

certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first a tactics, and narcotics training."

o, California Ballot Measure Would Reform Police Oversight, Accountability

ego Union-Tribune (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparen lity." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board wi aunch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained n in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "comp ns May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by n that they are guilty of misconduct."

IACP on June 24, 2020, at 1:00 p.m. EST for Part 2 and July 16, 2020, at 1:00 p.m. EST for Part 3 of *Mindfulness Strategies for Law ment* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety es Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim servi el, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute ve mindfulness sessions.

you space.

ect with the IACP online: **IACP Event Calendar:**

E & DRUGS

Rape Conviction Rates Rise 75% After Change In Law

(6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls r other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. U tries, prosecutors do not have to prove the use or threat of violence or coercion. The National Council on Crime Prevention (Bra) said the ris s – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected." According to Reuters, "Britain, Belgiu prus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Po ised similar reforms."

k City Raid Leads To Drug Seizures, Two Arrests

ork Post (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of "approximately 1.2 kilog grams of fentanyl and 2.3 kilograms of methamphetamine." Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who f criminal possession of a controlled substance and criminally using drug paraphernalia." The arrests were the result of joint operation condu Special Narcotics Prosecutor," the City of New York Police Department, and the DEA.

kers Barricade Themselves In Pub During Illegal Lockdown Lock-In

endent (UK) (6/22, Gregory) reports, "Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police break up the session, according to police." According to the Independent, "Merseyside Police officers were pelted with beer and other items ook up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered a ub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only 'a number of people' were said to take The Independent adds, "Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs

aw for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a
ures in place to protect customers."

NOLOGY

ks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers

(6/22, Taylor) reports hackers have "leaked highly sensitive police files from over 200 police departments across the country." Activist
s "published what the outlet calls 'hundreds of gigabytes' worth of potentially sensitive files' from police departments across the US." The gr
information dump 'BlueLeaks.'" The group "compiled the records, disseminating them into a searchable database that can pull up private in
ce badge number." Many of the files include "information such as memos, emails, and officers' personal information". The group "shared in
regarding the data dump."

AL SECURITY

Analysis: Antifa Rumors Show Ways Information Spreads Locally

ork Times (6/22, Alba, Decker) examines how in recent weeks, "residents in at least 41 U.S. cities and towns became alarmed by rumo
ollective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, th
their local law enforcement for help. In each case, it was for a threat that never appeared." On the local level, the analysis found that "the so
formation has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appea
Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking
nd community texting networks," which "can fall under the radar of the tech companies and online fact checkers."

Lives Matter Protests Spread To White, Rural Areas. The Wall Street Journal (6/22, Carlton, Subscription Publication) reports th
r racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

AY'S LEAD STORIES

ACP President Addresses Police Reform

orities Grapple With Illegal "Quarantine Raves"

efugee Arrested In UK Terrorist Attack That Left Three Dead

er Tools

e Email Address
eedback
scribe
Help
es

a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Poli
of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products
.

imentary copy of *The Lead* was sent to keith.morrison@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access
edia's privacy policy.

ation about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

al Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

© 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

FW: IACP's The Lead: Massachusetts Governor Seeks Training Bonuses For Police Officers

From:	Keith Morrison (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D2EBEC5431A14B10A53942341DBD54F4-KEITH MORRI>
To:	Kevin O'Donnell (Sheriff) <Kevin.Odonnell@cookcountyil.gov>
Sent:	June 23, 2020 6:52:01 AM CDT
Received:	June 23, 2020 6:52:00 AM CDT

From: The IACP [mailto:TheLead@iacp.bulletinmedia.com]
Sent: Tuesday, June 23, 2020 6:43 AM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Subject: IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

ith Morrison Tuesday, J

POLICING & POLICY

US Supreme Court Will Not Revisit Challenge To Qualified Immu Police

ABC News (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday off a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforc officers, despite intense national outcry over police misconduct and legal protect shield cops from liability. 'The Supreme Court has made clear that they are not pr reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert o doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 18 Americans the unambiguous ability to sue public officials over civil rights violation Supreme Court subsequently limited liability to only those rights that have becon established law.'"

Newsday (NY) (6/22, Brune) reports that qualified immunity "shields p from being sued for money damages in federal court for constitutional violations excessive force unless the officers broke any 'clearly established' law – a high bar plaintiffs to overcome." Newsday adds that police groups argue that ending quali 'would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retiremen ol of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a stateme

Democrats Threaten To Block GOP Police Reform Bill

(6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week essions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester thing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixin eader Schumer called the GOP bill "deeply and fundamentally flawed."

rs Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law. Reuters (6/22, Morgan) reports that the Sen "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is e cedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." How ys, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."

Find Recreational Marijuana Laws May Boost Traffic Deaths

(6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although quest out how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published rnal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an exc ths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change n state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalize al marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

ic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

ork Times (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury t een put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

usetts Governor Seeks Training Bonuses For Police Officers

(6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to $5,000 should they take on additional tr l filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize o the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law nt, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a

certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first a tactics, and narcotics training."

o, California Ballot Measure Would Reform Police Oversight, Accountability

ego Union-Tribune (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparen lity." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board wi aunch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained n in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "comp ns May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by n that they are guilty of misconduct."

IACP on June 24, 2020, at 1:00 p.m. EST for Part 2 and July 16, 2020, at 1:00 p.m. EST for Part 3 of *Mindfulness Strategies for Law ment* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety es Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim servi el, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute ve mindfulness sessions.

you space.

ect with the IACP online: **IACP Event Calendar:**

E & DRUGS

Rape Conviction Rates Rise 75% After Change In Law

(6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls r other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. U tries, prosecutors do not have to prove the use or threat of violence or coercion. The National Council on Crime Prevention (Bra) said the ris s – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected." According to Reuters, "Britain, Belgiu prus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Po ised similar reforms."

k City Raid Leads To Drug Seizures, Two Arrests

ork Post (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of "approximately 1.2 kilog grams of fentanyl and 2.3 kilograms of methamphetamine." Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who f criminal possession of a controlled substance and criminally using drug paraphernalia." The arrests were the result of joint operation condu Special Narcotics Prosecutor," the City of New York Police Department, and the DEA.

kers Barricade Themselves In Pub During Illegal Lockdown Lock-In

endent (UK) (6/22, Gregory) reports, "Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police break up the session, according to police." According to the Independent, "Merseyside Police officers were pelted with beer and other items ook up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered a ub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only 'a number of people' were said to take The Independent adds, "Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs

aw for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a
ures in place to protect customers."

NOLOGY

ks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers

(6/22, Taylor) reports hackers have "leaked highly sensitive police files from over 200 police departments across the country." Activist
s "published what the outlet calls 'hundreds of gigabytes' worth of potentially sensitive files' from police departments across the US." The gr
information dump 'BlueLeaks.'" The group "compiled the records, disseminating them into a searchable database that can pull up private in
ce badge number." Many of the files include "information such as memos, emails, and officers' personal information". The group "shared in
regarding the data dump."

AL SECURITY

Analysis: Antifa Rumors Show Ways Information Spreads Locally

ork Times (6/22, Alba, Decker) examines how in recent weeks, "residents in at least 41 U.S. cities and towns became alarmed by rumo
ollective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, th
their local law enforcement for help. In each case, it was for a threat that never appeared." On the local level, the analysis found that "the so
formation has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appea
Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking
nd community texting networks," which "can fall under the radar of the tech companies and online fact checkers."

Lives Matter Protests Spread To White, Rural Areas. The Wall Street Journal (6/22, Carlton, Subscription Publication) reports th
r racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

AY'S LEAD STORIES

ACP President Addresses Police Reform

orities Grapple With Illegal "Quarantine Raves"

efugee Arrested In UK Terrorist Attack That Left Three Dead

er Tools

e Email Address
eedback
scribe
Help
es

a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Poli
of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products
.

imentary copy of *The Lead* was sent to keith.morrison@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access
edia's privacy policy.

ation about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

al Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

© 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Cc: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Sent: June 23, 2020 7:02:37 AM CDT
Received: June 23, 2020 7:06:00 AM CDT

This is a different article from the International Association of Chief's of Police that relates Netsentinal is a Houston service provider for Law Enforcement.

https://www.theblaze.com/news/blueleaks-hackers-release-countless-records-on-police-officers-all-searchable-by-badge-number

From: Keith Morrison (Sheriff)
Sent: Tuesday, June 23, 2020 6:45 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

[redacted]

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:26 AM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Keith –

[redacted]

Doug

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 6:20 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM

To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

From:	Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Cc:	Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>, Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Sent:	June 23, 2020 7:10:54 AM CDT
Received:	June 23, 2020 7:10:56 AM CDT
Attachments:	report-workforce-software-2020-06-19.xlsx, report-workforce-software-2020-06-19.pdf

This is a different article from the International Association of Chiefs of Police that relates Netsentinal is a Houston service provider for Law Enforcement.

https://www.theblaze.com/news/blueleaks-hackers-release-countless-records-on-police-officers-all-searchable-by-badge-number

I think our only risk from doxing would be workforce. I pulled the attached reports last Friday and provided them to Chuck at Homeland for review.

From: Keith Morrison (Sheriff)
Sent: Tuesday, June 23, 2020 6:45 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

[redacted]

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:26 AM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Keith –

[redacted]

Doug

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 6:20 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

From:	Keith Morrison (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D2EBEC5431A14B10A53942341DBD54F4-KEITH MORRI>
Cc:	Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>, Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Sent:	June 23, 2020 7:10:54 AM CDT
Received:	June 23, 2020 7:10:00 AM CDT
Attachments:	report-workforce-software-2020-06-19.pdf, report-workforce-software-2020-06-19.xlsx

This is a different article from the International Association of Chiefs of Police that relates Netsentinal is a Houston service provider for Law Enforcement.

https://www.theblaze.com/news/blueleaks-hackers-release-countless-records-on-police-officers-all-searchable-by-badge-number

I think our only risk from doxing would be workforce. I pulled the attached reports last Friday and provided them to Chuck at Homeland for review.

From: Keith Morrison (Sheriff)
Sent: Tuesday, June 23, 2020 6:45 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

[redacted]

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:26 AM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Keith –

[redacted]

Doug

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 6:20 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

IT Security News Blast - 6-23-2020

From: Mike Hamilton <Michael.Hamilton@CI.Security>
To: Keith.Morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: June 23, 2020 7:14:12 AM CDT
Received: June 23, 2020 7:14:21 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

IT Security News Blast – 6-23-2020

Tomorrow, 6/24 - [WEBINAR] Mid-Pandemic Attacks and How to Thwart Them with MDR

There's still time to register for tomorrow's webinar at the MIDMRKT June virtual showcase! When organizations changed their work habits in unprecedented ways this year, they opened the door to significant cyber risks. Unfortunately, we are seeing those risks turn into exploited vulnerabilities now. In this webinar on Wednesday, June 24, InfoSec Veteran Mike Hamilton will show you what criminals are doing, how Managed Detection and Response can stop it, and what to do if you become the victim of a ransomware gang. It's free to register for tomorrow's hour-long event, starting at Noon ET/9am PT. Bring your questions for Q&A at the end.

https://virtual.midmrkt.com/s/virtual-technology-showcase-june2020

'BlueLeaks' Exposes Files from Hundreds of Police Departments

"Preliminary analysis of the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centers, law enforcement, and other

government agencies across the United States, was the source of the compromise," the NFCA wrote. "Netsential confirmed that this compromise was likely the result of a threat actor who leveraged a compromised Netsential customer user account and the web platform's upload feature to introduce malicious content, allowing for the exfiltration of other Netsential customer data."

https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

Oracle's BlueKai tracks you across the web. That data spilled online

Billions of records exposed.

Tech giant Oracle is one of a few companies in Silicon Valley that has near-perfected the art of tracking people across the internet. The company has spent a decade and billions of dollars buying startups to build its very own panopticon of users' web browsing data. [...] TechCrunch reviewed the data shared by Sen and found names, home addresses, email addresses and other identifiable data in the database. The data also revealed sensitive users' web browsing activity — from purchases to newsletter unsubscribes.

https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/?guccounter=1

Ransomware group auctions Crozer-Keystone Health System data on darknet

Netwalker, a ransomware operator that threatens to publish data online if ransoms aren't paid, hacked Springfield, Pa.-based Crozer-Keystone Health System and is auctioning off its data online, according to Cointelegraph. [...] Cointelegraph was able to access Netwalker's alleged publication on June 19, which showed "dozens of folders with an undisclosed amount of data, mostly concerning finances, but nothing related to medical records of patients," according to the report. Netwalker claimed Crozer-Keystone declined to pay for the ransom the group demanded in Bitcoin.

https://www.beckershospitalreview.com/cybersecurity/ransomware-group-auctions-crozer-keystone-health-system-data-on-darknet.html

Key cause of cyber loss identified in new report

“There is always going to be a human element, and it is impossible to get to 100% compliance with various rules, regulations and best practices,” said Mike Palotay, chief underwriting officer at Tokio Marine HCC. He pointed to the healthcare industry, which has a serious employee negligence risk because there are many people with access to private information that is being sent to different recipients.

https://www.insurancebusinessmag.com/us/news/cyber/key-cause-of-cyber-loss-identified-in-new-report-225838.aspx

Cybersecurity skills shortage amid attacks

"Traditionally we've done a lot of importing skills and that's been really fantastic to bring in experts in some of these areas. But that's not an option anymore - we have to grow these skills." Not-for-profit AustCyber's research predicts a shortage of 18,000 cyber experts by 2026. With unemployment on the rise during the pandemic, Ms Souness believes there's an opportunity to create jobs. "We've got hundreds of thousands of roles going, we've got new records in unemployment, if only we were upskilling people," Ms Souness said.

https://au.news.yahoo.com/cybersecurity-skills-shortage-amid-attacks-003800589--spt.html

Why SMEs are increasing their cyber insurance budgets

Research has also suggested cybercriminals view SMEs as possible entry points to gain access to the network of a larger company. Often, the damage and recovery costs of businesses having to deal with the aftermath of malicious attacks leads to not only plummet productivity, but in some cases, to deteriorating trust between firm and clients.

https://techhq.com/2020/06/why-smes-are-increasing-budgets-for-cyber-insurance/

Companies are rethinking their approach to privacy management

Twenty-two percent of respondents said personal device security during the pandemic has added a great deal of risk to their businesses. “Personal device security” received the highest proportion of “a great deal of risk” responses,

compared to the other four response options.

A majority of respondents said that third-party data, supply chain, personal-device security, unintentional data sharing, and required or voluntary data sharing for public health purposes all added at least a moderate amount of risk to their businesses.

https://www.helpnetsecurity.com/2020/06/22/privacy-management/

Addressing Cybersecurity in The Time Of COVID-19 and Beyond

· An enterprise-wide strategic risk. Although there is an IT component, cybersecurity is not just an IT problem. It is also a human resource issue and a financial issue, so it should be woven into the business.

· Legal and disclosure implications. Boards need to be aware of their unique legal obligations, which vary from country to country and by sector.

· Board oversight structure and access to expertise. To create an effective cybersecurity strategy, boards need to bring in outside cyber and privacy experts.

· An enterprise framework for managing cyber risk. Boards and management across the enterprise must work together in developing a cyber strategy, as well as understand each other's roles.

[...]

https://www.financialexecutives.org/FEI-Daily/June-2020/Addressing-Cybersecurity-in-The-Time-Of-COVID-19-a.aspx

Government groups work together to mitigate cybersecurity risks in solar development

The rapid growth and importance of solar energy has elevated the critical need among state-level decision makers to evaluate the potential cybersecurity implications of solar deployment and work with federal and private-sector stakeholders to mitigate those risks. Newer two-way communication technologies and remote grid support are revolutionizing how the grid operates, but also result in a system more exposed to cyber vulnerabilities. NASEO and NARUC seek to proactively address cyber threats in all energy areas, including solar infrastructure.

https://www.solarpowerworldonline.com/2020/06/government-groups-partner-to-mitigate-cybersecurity-risks-in-solar-development/

Power transformers and Aurora

In general if we want to attack substation functions, there are a few options in diagram 1. The attack can come over the network, the SCADA is frequently connected to the corporate network or even to the Internet. Famous example is the Ukraine attack on the power distribution. We can try penetrating the WAN, these are not always private connections so there are opportunities here. So far never seen an example of this. And we can attack the time source, time is a very important element in the control of a power system.

https://otcybersecurity.blog/2020/06/20/power-transformers-and-aurora/

During global pandemic, USCYBERCOM trains virtually to defend networks, protect nation

Over the period of two weeks, Cyber Flag 20-2 will host more than 500 personnel worldwide, spanning across nine different time zones and 17 cyber teams. Participants include three allied nations, the Air National Guard, the Coast Guard, the U.S. Army Corps of Engineers, U.S. Postal Service, U.S. Dept. of Energy and multiple service cyber components across the DOD.

https://www.cybercom.mil/Media/News/Article/2227651/during-global-pandemic-uscybercom-trains-virtually-to-defend-networks-protect-n/

Key Solarium recommendations find a home in the defense bill

The Subcommittee on Intelligence and Emerging Threats adopted a markup June 22 that includes provisions directing the Department of Defense to assess the national security risks posed by quantum computing, assess the impact of greater private-public collaboration between government and critical infrastructure owners and operators, clarify the cybersecurity capabilities and interoperability of the National Guard and expanding a program authorizing DOD employees to use paid leave for cybersecurity education.

https://fcw.com/articles/2020/06/22/johnson-solarium-ndaa-markup-emerging.aspx

Estonia's Crucial Role in Tackling Growing Cyber Threats

The lesson from Estonia for any country wishing to undergo digital transformation is simple – that threats to peace and security in the physical world can be translated to cyberspace. Through developing its cyber incident response, the government's own cyber security capacity and its digital infrastructure, Estonia became a model and a leader on digitization and e-governance efforts. And although those involved in developing the governance of cyberspace pay credence to a multi-stakeholder approach - involving actors from the private sector, technical community, civil society and academia - states remain the key players.

https://www.chathamhouse.org/expert/comment/estonia-s-crucial-role-tackling-growing-cyber-threats#

Does a generalization of tracking data cover up our traces on the internet?

Many providers of tracking services advertise secure data protection by generalizing datasets and anonymizing data in this way. [...] Strufe, together with his team and colleagues of TUD, have now studied whether this method really allows no conclusions to be drawn with respect to the individual. With the help of a large volume of metadata of German websites with 66 million users and over 2 billion page views, the computer scientists succeeded in not only drawing conclusions with respect to the websites accessed, but also with respect to the chains of page views, the so-called click traces.

https://www.helpnetsecurity.com/2020/06/22/generalization-of-tracking-data/

Privacy experts say many coronavirus apps aren't doing enough to safeguard users' information [Subscription]

Developers of the apps, researchers say, did not implement strong digital protections that are standard on other technology that deals with sensitive personal or health information And many are siphoning data to third parties — which means peoples' private information could be used for targeted advertising or to track them across

other, non-related apps.

https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/06/22/the-cybersecurity-202-privacy-experts-say-many-coronavirus-apps-aren-t-doing-enough-to-safeguard-users-information/5eefae20602ff12947e91075/

Crooks abuse Google Analytics to conceal theft of payment card data

One challenge in pulling off the hack is bypassing website security policies or concealing the exfiltration of massive amounts of sensitive data from endpoint security applications installed on the infected network. Researchers from Kaspersky Lab on Monday said that they have recently observed about two dozen infected sites that found a novel way to achieve this. Instead of sending it to attacker-controlled servers, the attackers send it to Google Analytics accounts they control. Since the Google service is so widely used, ecommerce site security policies generally fully trust it to receive data.

https://arstechnica.com/information-technology/2020/06/google-analytics-trick-allows-crooks-to-hide-card-skimming/

AMD: Fixes For High-Severity SMM Callout Flaws Upcoming

“AMD is aware of new research related to a potential vulnerability in AMD software technology supplied to motherboard manufacturers for use in their Unified Extensible Firmware Interface (UEFI) infrastructure and plans to complete delivery of updated versions designed to mitigate the issue by the end of June 2020,” according to AMD.

https://threatpost.com/amd-fixes-for-high-severity-smm-callout-flaws-upcoming/156787/

Elon Musk invites users to test Starlink space internet

The $36 billion company now has over 500 satellites in orbit. Last week it announced that trials of its space-based Internet platform could start within weeks. An invitation to sign up for Starlink updates was published on the startup’s website. Users sign up with an email address and zip code, and are told Starlink will begin beta-testing this summer in the Northern hemisphere. The company promises to notify everyone with

the right zip code if trials are going on in their area.

https://decrypt.co/33080/elon-musk-invites-users-to-test-starlink-space-internet

You are receiving this email because you are subscribed to receive the IT Security Daily Blast email from Michael Hamilton, Founder, President, and CISO of CI Security, formerly Critical Informatics.

Archived articles are available at https://ci.security/news/daily-news.

CI Security and the CI Security logo are the trademarks of CI Security, Inc. All other brand names, trademarks, service marks, and copyrights are the property of their respective owners.

© 2020 CI Security. All rights reserved.

CI Security

245 4th St, Suite 405 Bremerton, WA 98337

IT Security News Blast - 6-23-2020

From: Mike Hamilton <Michael.Hamilton@CI.Security>
To: christopher.moore@cookcountyil.gov, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>

Sent: June 23, 2020 7:14:12 AM CDT
Received: June 23, 2020 7:14:24 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

IT Security News Blast – 6-23-2020

Tomorrow, 6/24 - [WEBINAR] Mid-Pandemic Attacks and How to Thwart Them with MDR

There's still time to register for tomorrow's webinar at the MIDMRKT June virtual showcase! When organizations changed their work habits in unprecedented ways this year, they opened the door to significant cyber risks. Unfortunately, we are seeing those risks turn into exploited vulnerabilities now. In this webinar on Wednesday, June 24, InfoSec Veteran Mike Hamilton will show you what criminals are doing, how Managed Detection and Response can stop it, and what to do if you become the victim of a ransomware gang. It's free to register for tomorrow's hour-long event, starting at Noon ET/9am PT. Bring your questions for Q&A at the end.

https://virtual.midmrkt.com/s/virtual-technology-showcase-june2020

'BlueLeaks' Exposes Files from Hundreds of Police Departments

"Preliminary analysis of the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centers, law enforcement, and other

government agencies across the United States, was the source of the compromise," the NFCA wrote. "Netsential confirmed that this compromise was likely the result of a threat actor who leveraged a compromised Netsential customer user account and the web platform's upload feature to introduce malicious content, allowing for the exfiltration of other Netsential customer data."

https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

Oracle's BlueKai tracks you across the web. That data spilled online

Billions of records exposed.

Tech giant Oracle is one of a few companies in Silicon Valley that has near-perfected the art of tracking people across the internet. The company has spent a decade and billions of dollars buying startups to build its very own panopticon of users' web browsing data. [...] TechCrunch reviewed the data shared by Sen and found names, home addresses, email addresses and other identifiable data in the database. The data also revealed sensitive users' web browsing activity — from purchases to newsletter unsubscribes.

https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/?guccounter=1

Ransomware group auctions Crozer-Keystone Health System data on darknet

Netwalker, a ransomware operator that threatens to publish data online if ransoms aren't paid, hacked Springfield, Pa.-based Crozer-Keystone Health System and is auctioning off its data online, according to Cointelegraph. [...] Cointelegraph was able to access Netwalker's alleged publication on June 19, which showed "dozens of folders with an undisclosed amount of data, mostly concerning finances, but nothing related to medical records of patients," according to the report. Netwalker claimed Crozer-Keystone declined to pay for the ransom the group demanded in Bitcoin.

https://www.beckershospitalreview.com/cybersecurity/ransomware-group-auctions-crozer-keystone-health-system-data-on-darknet.html

Key cause of cyber loss identified in new report

“There is always going to be a human element, and it is impossible to get to 100% compliance with various rules, regulations and best practices,” said Mike Palotay, chief underwriting officer at Tokio Marine HCC. He pointed to the healthcare industry, which has a serious employee negligence risk because there are many people with access to private information that is being sent to different recipients.

https://www.insurancebusinessmag.com/us/news/cyber/key-cause-of-cyber-loss-identified-in-new-report-225838.aspx

Cybersecurity skills shortage amid attacks

"Traditionally we've done a lot of importing skills and that's been really fantastic to bring in experts in some of these areas. But that's not an option anymore - we have to grow these skills." Not-for-profit AustCyber's research predicts a shortage of 18,000 cyber experts by 2026. With unemployment on the rise during the pandemic, Ms Souness believes there's an opportunity to create jobs. "We've got hundreds of thousands of roles going, we've got new records in unemployment, if only we were upskilling people," Ms Souness said.

https://au.news.yahoo.com/cybersecurity-skills-shortage-amid-attacks-003800589--spt.html

Why SMEs are increasing their cyber insurance budgets

Research has also suggested cybercriminals view SMEs as possible entry points to gain access to the network of a larger company. Often, the damage and recovery costs of businesses having to deal with the aftermath of malicious attacks leads to not only plummet productivity, but in some cases, to deteriorating trust between firm and clients.

https://techhq.com/2020/06/why-smes-are-increasing-budgets-for-cyber-insurance/

Companies are rethinking their approach to privacy management

Twenty-two percent of respondents said personal device security during the pandemic has added a great deal of risk to their businesses. “Personal device security” received the highest proportion of “a great deal of risk” responses,

compared to the other four response options.

A majority of respondents said that third-party data, supply chain, personal-device security, unintentional data sharing, and required or voluntary data sharing for public health purposes all added at least a moderate amount of risk to their businesses.

https://www.helpnetsecurity.com/2020/06/22/privacy-management/

Addressing Cybersecurity in The Time Of COVID-19 and Beyond

· An enterprise-wide strategic risk. Although there is an IT component, cybersecurity is not just an IT problem. It is also a human resource issue and a financial issue, so it should be woven into the business.

· Legal and disclosure implications. Boards need to be aware of their unique legal obligations, which vary from country to country and by sector.

· Board oversight structure and access to expertise. To create an effective cybersecurity strategy, boards need to bring in outside cyber and privacy experts.

· An enterprise framework for managing cyber risk. Boards and management across the enterprise must work together in developing a cyber strategy, as well as understand each other's roles.

[...]

https://www.financialexecutives.org/FEI-Daily/June-2020/Addressing-Cybersecurity-in-The-Time-Of-COVID-19-a.aspx

Government groups work together to mitigate cybersecurity risks in solar development

The rapid growth and importance of solar energy has elevated the critical need among state-level decision makers to evaluate the potential cybersecurity implications of solar deployment and work with federal and private-sector stakeholders to mitigate those risks. Newer two-way communication technologies and remote grid support are revolutionizing how the grid operates, but also result in a system more exposed to cyber vulnerabilities. NASEO and NARUC seek to proactively address cyber threats in all energy areas, including solar infrastructure.

https://www.solarpowerworldonline.com/2020/06/government-groups-partner-to-mitigate-cybersecurity-risks-in-solar-development/

Power transformers and Aurora

In general if we want to attack substation functions, there are a few options in diagram 1. The attack can come over the network, the SCADA is frequently connected to the corporate network or even to the Internet. Famous example is the Ukraine attack on the power distribution. We can try penetrating the WAN, these are not always private connections so there are opportunities here. So far never seen an example of this. And we can attack the time source, time is a very important element in the control of a power system.

https://otcybersecurity.blog/2020/06/20/power-transformers-and-aurora/

During global pandemic, USCYBERCOM trains virtually to defend networks, protect nation

Over the period of two weeks, Cyber Flag 20-2 will host more than 500 personnel worldwide, spanning across nine different time zones and 17 cyber teams. Participants include three allied nations, the Air National Guard, the Coast Guard, the U.S. Army Corps of Engineers, U.S. Postal Service, U.S. Dept. of Energy and multiple service cyber components across the DOD.

https://www.cybercom.mil/Media/News/Article/2227651/during-global-pandemic-uscybercom-trains-virtually-to-defend-networks-protect-n/

Key Solarium recommendations find a home in the defense bill

The Subcommittee on Intelligence and Emerging Threats adopted a markup June 22 that includes provisions directing the Department of Defense to assess the national security risks posed by quantum computing, assess the impact of greater private-public collaboration between government and critical infrastructure owners and operators, clarify the cybersecurity capabilities and interoperability of the National Guard and expanding a program authorizing DOD employees to use paid leave for cybersecurity education.

https://fcw.com/articles/2020/06/22/johnson-solarium-ndaa-markup-emerging.aspx

Estonia's Crucial Role in Tackling Growing Cyber Threats

The lesson from Estonia for any country wishing to undergo digital transformation is simple – that threats to peace and security in the physical world can be translated to cyberspace. Through developing its cyber incident response, the government's own cyber security capacity and its digital infrastructure, Estonia became a model and a leader on digitization and e-governance efforts. And although those involved in developing the governance of cyberspace pay credence to a multi-stakeholder approach - involving actors from the private sector, technical community, civil society and academia - states remain the key players.

https://www.chathamhouse.org/expert/comment/estonia-s-crucial-role-tackling-growing-cyber-threats#

Does a generalization of tracking data cover up our traces on the internet?

Many providers of tracking services advertise secure data protection by generalizing datasets and anonymizing data in this way. [...] Strufe, together with his team and colleagues of TUD, have now studied whether this method really allows no conclusions to be drawn with respect to the individual. With the help of a large volume of metadata of German websites with 66 million users and over 2 billion page views, the computer scientists succeeded in not only drawing conclusions with respect to the websites accessed, but also with respect to the chains of page views, the so-called click traces.

https://www.helpnetsecurity.com/2020/06/22/generalization-of-tracking-data/

Privacy experts say many coronavirus apps aren't doing enough to safeguard users' information [Subscription]

Developers of the apps, researchers say, did not implement strong digital protections that are standard on other technology that deals with sensitive personal or health information And many are siphoning data to third parties — which means peoples' private information could be used for targeted advertising or to track them across

other, non-related apps.

https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/06/22/the-cybersecurity-202-privacy-experts-say-many-coronavirus-apps-aren-t-doing-enough-to-safeguard-users-information/5eefae20602ff12947e91075/

Crooks abuse Google Analytics to conceal theft of payment card data

One challenge in pulling off the hack is bypassing website security policies or concealing the exfiltration of massive amounts of sensitive data from endpoint security applications installed on the infected network. Researchers from Kaspersky Lab on Monday said that they have recently observed about two dozen infected sites that found a novel way to achieve this. Instead of sending it to attacker-controlled servers, the attackers send it to Google Analytics accounts they control. Since the Google service is so widely used, ecommerce site security policies generally fully trust it to receive data.

https://arstechnica.com/information-technology/2020/06/google-analytics-trick-allows-crooks-to-hide-card-skimming/

AMD: Fixes For High-Severity SMM Callout Flaws Upcoming

“AMD is aware of new research related to a potential vulnerability in AMD software technology supplied to motherboard manufacturers for use in their Unified Extensible Firmware Interface (UEFI) infrastructure and plans to complete delivery of updated versions designed to mitigate the issue by the end of June 2020,” according to AMD.

https://threatpost.com/amd-fixes-for-high-severity-smm-callout-flaws-upcoming/156787/

Elon Musk invites users to test Starlink space internet

The $36 billion company now has over 500 satellites in orbit. Last week it announced that trials of its space-based Internet platform could start within weeks. An invitation to sign up for Starlink updates was published on the startup’s website. Users sign up with an email address and zip code, and are told Starlink will begin beta-testing this summer in the Northern hemisphere. The company promises to notify everyone with

the right zip code if trials are going on in their area.

https://decrypt.co/33080/elon-musk-invites-users-to-test-starlink-space-internet

You are receiving this email because you are subscribed to receive the IT Security Daily Blast email from Michael Hamilton, Founder, President, and CISO of CI Security, formerly Critical Informatics.

Archived articles are available at https://ci.security/news/daily-news.

CI Security and the CI Security logo are the trademarks of CI Security, Inc. All other brand names, trademarks, service marks, and copyrights are the property of their respective owners.

© 2020 CI Security. All rights reserved.

CI Security

245 4th St, Suite 405 Bremerton, WA 98337

RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

From: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: June 23, 2020 7:17:01 AM CDT
Received: June 23, 2020 7:17:03 AM CDT

Thanks.

Douglas MacLean
Deputy CIO, BOIT
Cook County Sheriff's Office
South Campus, Building 1
3rd Floor
Chicago, IL 60608

773.674.8615 [d]
312.877.2048 [c]

From Mobile

-------- Original message --------
From: "Keith Morrison (Sheriff)" <Keith.Morrison@cookcountyil.gov>
Date: 6/23/20 06:45 (GMT-06:00)
To: "Douglas Maclean (Sheriff)" <Douglas.Maclean2@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

[redacted]

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:26 AM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Keith –

[redacted]

Doug

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 6:20 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

[Anomali ThreatStream] Your daily Threat Model digest

From: Anomali ThreatStream <info@anomali.com>
To: keith.morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: June 23, 2020 8:26:41 AM CDT
Received: June 23, 2020 8:26:47 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Threat Model Daily Digest (June 23)

- New Signature rule crime_win32_ransomexx_locker__dot_1
- New TTP Exploit Database: [dos] Frigate 2.02 - Denial Of Service (PoC)
- New TTP Exploit Database: [webapps] Online Student Enrollment System 1.0 - Unauthenticated Arbitrary File Upload
- New TTP Exploit Database: [webapps] WebPort 1.19.1 - 'setup' Reflected Cross-Site Scripting
- New TTP Exploit Database: [webapps] WebPort 1.19.1 - Reflected Cross-Site Scripting
- New TTP Exploit Database: [webapps] Student Enrollment 1.0 - Unauthenticated Remote Code Execution
- New TTP Exploit Database: [webapps] Odoo 12.0 - Local File Inclusion
- New TTP bugbountywriteup: API Token Hijacking Through Clickjacking
- New Zero Day Initiative: Our CVE Story: Bringing our ZDI community to the CVE community
- New CISA Bulletins: Vulnerability Summary for the Week of June 15 2020
- New TTP PhishLabs: Executive Impersonation Techniques on Social Media
- New TTP Exploit Database: [webapps] FileRun 2019.05.21 - Reflected Cross-Site Scripting
- New TTP Sophos Naked Security: Anatomy of a survey scam – how innocent questions can rip you off
- New Threat Bulletin 2 updates: Bleeping Computer: Indiabulls Group hit by CLOP Ransomware gets 24h leak deadline - hxxps://www[.]bleepingcomputer[.]com/news/security/ind... created by Chris Collins
- New Threat Bulletin 2 updates: Akamai Security Intel: Akamai Mitigates Sophisticated 1.44 Tbps and 385 Mpps DDoS Attack - The Akamai Blog - hxxps://blogs[.]akamai[.]com/2020/06/akamai-mitigates-... created by Chris Collins
- New Threat Bulletin 2 updates: Threatpost: Report: 'BlueLeaks' Exposes Sensitive Data From Police Departments - hxxps://threatpost[.]com/report-blueleaks-exposes-se... created by Chris Collins
- New Threat Bulletin 2 updates: Bleeping Computer: Hackers use Google Analytics to steal credit cards bypass CSP - hxxps://www[.]bleepingcomputer[.]com/news/security/hac... created by Chris Collins
- New Threat Bulletin 4 updates: arxiv[.]org: 2005.08208 - LostandFound:StoppingBluetoothFindersfrom LeakingP... created by Chris Collins

- New Threat Bulletin 3 updates: # security[.]neurolabs: Comparative analysis between Bindiff and Diaphora - Patched Smokeloader Study Case - hxxp://security[.]neurolabs[.]club/2020/04/diffing-mal... created by Chris Collins
- New Threat Bulletin 3 updates: Popular MMO game Stalker Online hacked, 1.2 million user records put for sale on hacker forums | CyberNews - In the News Careers Contact Send Us a Tip NEWSLETT... created by ebrady(at)firstenergycorp[.]com
- New Threat Bulletin 2 updates: Sucuri: Cross Site Scripting in YITH WooCommerce Ajax Product Filter - hxxps://blog[.]sucuri[.]net/2020/06/cross-site-scripti... created by Chris Collins
- New Threat Bulletin 2 updates: Maersk, me & notPetya - gvnshtn | Threat Bulletin Created on 2020-06-22 19:09:25 - Original source: hxxps://gvnshtn[.]com/maersk-me- not... created by Neil Finneran
- New Threat Bulletin 3 updates: Cisco Talos: IndigoDrop spreads via military-themed lures to deliver Cobalt Strike - hxxps://blog[.]talosintelligence[.]com/2020/06/indigod... created by Chris Collins
- New Threat Bulletin 3 updates: Forescout: EKANS Strikes Again: Honda and Enel Taken Down by Ransomware - hxxps://www[.]forescout[.]com/company/blog/ekans-strik... created by Chris Collins
- New Threat Bulletin 3 updates: Trustwave: Pillowmint: FIN7's Monkey Thief - hxxps://www[.]trustwave[.]com /en-us/resources/blogs/sp... created by Chris Collins
- New Threat Bulletin 2 updates: We found 6 critical PayPal vulnerabilities - and PayPal punished us for it | CyberNews | Threat Bulletin Created on 2020-06-22 18:04:50 - Original source: hxxps://cybernews[.]com/security/we... created by Chad Colbetzor
- New Threat Bulletin 4 updates: ssi[.]gouv[.]fr: CERTFR 2020 CTI 006 - TLP:WHITE ÉVOLUTIONDEL'ACTIVITÉDU GROUPECYBERCRIMI... created by Chris Collins
- New Threat Bulletin 2 updates: ssi[.]gouv[.]fr: CERTFR-2020-CTI-006 : Évolution de l'activité du groupe cybercriminel TA505 (22 juin 2020) - hxxps://www[.]cert[.]ssi[.]gouv[.]fr/cti/CERTFR-2020-CTI-0... created by Chris Collins
- New Threat Bulletin 2 updates: SC Media: Don't be the weakest link in a widespread attack - hxxps://www[.]scmagazine[.]com/infosec-world-2020/dont... created by Chris Collins
- New Threat Bulletin 2 updates: Cyjax: Geopolitical and Cybersecurity Weekly – 15 June 2020 - hxxps://www[.]cyjax[.]com/2020/06/15/geopolitical-and-... created by Chris Collins
- New Threat Bulletin 3 updates: Sentinel One Security Research: Inside a TrickBot Cobalt Strike Attack Server - hxxps://labs[.]sentinelone[.]com/inside-a-trickbot-cob... created by Chris Collins
- New Threat Bulletin 3 updates: Anomali Community Threat Briefing: 2020-06-22 - Weekly Threat Briefing: APT Group, Cobalt, COVID-1... created by Tara Gould
- New Threat Bulletin 2 updates: cyberscoop: Here's what John Bolton had to say about cybersecurity policy in his new book - hxxps://www[.]cyberscoop[.]com/john-bolton-book- cybers... created by Chris Collins
- New Threat Bulletin 3 updates: ssi[.]gouv[.]fr: CERTFR-2020-IOC-004 : Le groupe cybercriminel TA505 (22 juin 2020) - hxxps://www[.]cert[.]ssi[.]gouv[.]fr/ioc/CERTFR-2020-IOC-0... created by Chris Collins

- Threat Bulletin 2 updates: Securelist / Kaspersky: Web skimming with Google Analytics - hxxps://securelist[.]com/web-skimming-with-google-an... created by Chris Collins
- Threat Bulletin 1 update: Krebs on Security: 'BlueLeaks' Exposes Files from Hundreds of Police Departments - hxxps://krebsonsecurity[.]com/2020/06/blueleaks-expo... created by Chris Collins
- Threat Bulletin 2 updates: Malware Traffic Analysis: 2020-06-17 - Qakbot (Qbot) spx142 infection - hxxps://www[.]malware-traffic-analysis[.]net/2020/06/1... created by Chris Collins
- Threat Bulletin 1 update: Underground Pulse - June 15, 2020 - Underground Pulse - June 15, 2020 Document Family:... created by Intel 471

To unsubscribe from these notifications, go to https://ccctig.threatstream.com/settings.

Thank you!

Copyright 2020 Anomali, Inc.

ISN Digest, Vol 52, Issue 8

From: isn-request@lists.infosecnews.org
To: isn@lists.infosecnews.org
Sender: ISN <isn-bounces@lists.infosecnews.org>
Sent: June 23, 2020 11:00:02 AM CDT
Received: June 23, 2020 11:00:28 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Send ISN mailing list submissions to
isn@lists.infosecnews.org

To subscribe or unsubscribe via the World Wide Web, visit
http://lists.infosecnews.org/mailman/listinfo/isn_lists.infosecnews.org

or, via email, send a message with subject or body 'help' to
isn-request@lists.infosecnews.org

You can reach the person managing the list at
isn-owner@lists.infosecnews.org

When replying, please edit your Subject line so it is more specific
than "Re: Contents of ISN digest..."

Today's Topics:

1. BlueLeaks: Data from 200 US police departments & fusion
centers published online (InfoSec News)
2. Microsoft acquires industrial cybersecurity startup CyberX
for $165M (InfoSec News)
3. House bill charges Guard, Reserve forces with defending the
nation in cyberspace (InfoSec News)
4. Here's what John Bolton had to say about cybersecurity policy
in his new book (InfoSec News)
5. 'Off limits': Australia, US urged to name and shame cyber
attackers targeting health research (InfoSec News)

Message: 1
Date: Tue, 23 Jun 2020 06:20:22 +0000 (UTC)
From: InfoSec News <alerts@infosecnews.org>
To: isn@lists.infosecnews.org
Subject: [ISN] BlueLeaks: Data from 200 US police departments & fusion
centers published online
Message-ID:
<alpine.DEB.2.21.2006230620060.9634@ip-172-30-0-239.ec2.internal>

Content-Type: text/plain; charset=US-ASCII; format=flowed

https://www.zdnet.com/article/blueleaks-data-from-200-us-police-departments-fusion-centers-published-online/

By Catalin Cimpanu
Zero Day
ZDNet.com
June 22, 2020

An activist group has published on Friday 296 GB of data they claim have been stolen from US law enforcement agencies and fusion centers.

The files, dubbed BlueLeaks, have been published by Distributed Denial of Secrets (DDoSecrets), a group that describes itself as a "transparency collective."

The data has been made available online on a searchable portal. According to the BlueLeaks portal, the leaked data contains more than one million files, such as scanned documents, videos, emails, audio files, and more.

DDoSecrets claims the leaked files contain more than ten years-worth of files belonging to more than 200 police departments and law enforcement fusion centers from across the US.

[...]

Message: 2
Date: Tue, 23 Jun 2020 06:20:35 +0000 (UTC)
From: InfoSec News <alerts@infosecnews.org>
To: isn@lists.infosecnews.org
Subject: [ISN] Microsoft acquires industrial cybersecurity startup CyberX for $165M
Message-ID: <alpine.DEB.2.21.2006230620230.9634@ip-172-30-0-239.ec2.internal>
Content-Type: text/plain; charset="utf-8"; Format="flowed"

https://siliconangle.com/2020/06/22/microsoft-acquires-industrial-cybersecurity-startup-cyberx-165m/

By Duncan Riley
Silicon Angle
June 22, 2020

Microsoft Corp. has acquired industrial cybersecurity startup CyberX Inc. for an undisclosed sum.

Various reports today suggest that the acquisition price was $165 million, following initial reports of the deal in May.

Founded in 2013, CyberX offers an industrial cybersecurity platform built by

former military cybersecurity experts with nation-state expertise defending critical infrastructure. The company?s platform focuses on continuously reducing industrial control systems risk and preventing costly production outages, safety failures and environmental incidents.

The company?s platform works by mapping out all connected devices in a factory or corporate network to give administrators a high-level view of potential risks. CyberX displays unmanaged systems and equipment running on outdated firmware as well as detecting malware. Its detection algorithms are said to spot threats by looking for system activity that deviates from a device?s normal behavior.

CyberX?s platform integrates with customers? existing information technology security stacks, including Splunk, IBM Security, Palo Alto Networks, Cisco Systems, RSA NetWitness and ServiceNow.

[...]

Message: 3
Date: Tue, 23 Jun 2020 06:20:49 +0000 (UTC)
From: InfoSec News <alerts@infosecnews.org>
To: isn@lists.infosecnews.org
Subject: [ISN] House bill charges Guard, Reserve forces with defending the nation in cyberspace
Message-ID: <alpine.DEB.2.21.2006230620370.9634@ip-172-30-0-239.ec2.internal>
Content-Type: text/plain; charset="utf-8"; Format="flowed"

https://www.fifthdomain.com/congress/2020/06/22/house-bill-charges-guard-reserve-forces-with-defending-the-nation-in-cyberspace/

By Mark Pomerleau
Fifth Domain
June 22, 2020

A House Armed Services Committee draft of the annual defense policy bill calls for the National Guard and Reserve components to assist in defending the nation in cyberspace.

A provision in the bill?s markup from the Subcommittee on Intelligence and Emerging Threats and Capabilities, which passed the committee June 22, requires a review of statues and rules that pertain to the use of the National Guard for response and recovery from significant cyberattacks.

The bill defines a cyber incident as significant if the event results in demonstrable harm to the national security interests or economy of the United States and the public confidence, civil liberties, or public health and safety of the American people.

A separate provision in the bill requires an evaluation of nontraditional cyber support to the Department of Defense. The assessment will include an evaluation of Reserve and Guard support to cyber operations forces; an evaluation of various Reserve, Guard, auxiliary and nontraditional support models to include those that can be utilized domestically and internationally; and an evaluation of dedicated reserve components specific to U.S. Cyber Command.

[...]

Message: 4
Date: Tue, 23 Jun 2020 06:21:05 +0000 (UTC)
From: InfoSec News <alerts@infosecnews.org>
To: isn@lists.infosecnews.org
Subject: [ISN] Here's what John Bolton had to say about cybersecurity policy in his new book
Message-ID: <alpine.DEB.2.21.2006230620520.9634@ip-172-30-0-239.ec2.internal>
Content-Type: text/plain; charset="utf-8"; Format="flowed"

https://www.cyberscoop.com/john-bolton-book-cybersecurity-nspm-13-crowdstrike/

By Shannon Vavra
CYBERSCOOP
June 22, 2020

In his new book, former national security adviser John Bolton says that squabbling amongst Trump administration officials hobbled the White House?s efforts to issue new policies that shaped the U.S. government?s offensive and defense cyber-operations.

The book, ?The Room Where It Happened: A White House Memoir,? which CyberScoop obtained, provides an insider?s view of the U.S. government?s largely secretive approach to revamping cyber policy in the last two years. Aside from cyber-operations, Bolton paints President Donald Trump as preoccupied and angered by cybersecurity-related issues, as well as all too willing to use hacking to prop up his political goals in negotiations with China and Ukraine.

?We needed to do two things: first, we needed a Trump Administration cyber strategy, and second, we needed to scrap the Obama-era [offensive cyber-operations] rules and replace them with a more agile, expeditious decision-making structure,? Bolton writes of his time negotiating new policies with national security and intelligence officials in 2018. ?Unfortunately, bureaucratic inertia, turf fights, and some genuine unresolved issues paralyzed the Trump Administration, month after month.?

Bolton writes that the Obama administration?s approach to fending off hacking from China, Russia, Iran, and North Korea had been criticized for not being aggressive enough. In order to better deter them, the Trump administration had set its sights on giving U.S. military hackers more leeway to hit back.

[...]

Message: 5
Date: Tue, 23 Jun 2020 06:21:19 +0000 (UTC)
From: InfoSec News <alerts@infosecnews.org>
To: isn@lists.infosecnews.org
Subject: [ISN] 'Off limits': Australia, US urged to name and shame
cyber attackers targeting health research
Message-ID:
<alpine.DEB.2.21.2006230621070.9634@ip-172-30-0-239.ec2.internal>
Content-Type: text/plain; charset=US-ASCII; format=flowed

https://www.smh.com.au/politics/federal/off-limits-australia-us-urged-to-name-and-shame-cyber-attackers-targeting-health-research-20200622-p554xo.html

By Anthony Galloway
Sydney Morning Herald
June 23, 2020

Australia and the United States have been urged to jointly name and shame state-backed actors looking to steal health research during the coronavirus pandemic, as the Morrison government battles an escalation in cyber attacks on key networks.

In a paper to be published by the United States Studies Centre at the University of Sydney on Tuesday, five foreign policy experts also say the two countries should strengthen their ability to counter disinformation campaigns as an urgent priority in light of China's use of such tactics during COVID-19.

Australian security agencies believe China is responsible for a wave of cyber attacks against the NSW government and other critical Australian infrastructure including state-owned utilities and hospitals but the Morrison government has chosen not to name the country involved.

While China has denied it is behind the Australian attacks, the US recently warned Beijing's most skilled hackers and spies were working to steal American research to develop vaccines and treatments for COVID-19.

[...]

Subject: Digest Footer

--
Subscribe to InfoSec News
https://www.infosecnews.org/subscribe-to-infosec-news/
https://twitter.com/infosecnews_

End of ISN Digest, Vol 52, Issue 8

Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

To:	Michael Aliperti, Ben Spear
Sent:	June 23, 2020 11:03:42 AM CDT
Received:	June 23, 2020 11:10:08 AM CDT

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Scott.Lefko@cookcountyil.gov, Scott Lefko (Sheriff) <Scott.Lefko@cookcountyil.gov>

Sent: June 23, 2020 3:22:00 PM CDT
Received: June 23, 2020 3:22:51 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: joseph.scofield@cookcountyil.gov, Joseph Scofield (Sheriff) <Joseph.Scofield@cookcountyil.gov>

Sent: June 23, 2020 3:22:00 PM CDT
Received: June 23, 2020 3:22:18 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: theodore.stajura@cookcountyil.gov, Theodore Stajura (Sheriff) <Theodore.Stajura@cookcountyil.gov>

Sent: June 23, 2020 3:22:00 PM CDT
Received: June 23, 2020 3:22:16 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: martin.bennett@cookcountyil.gov, Martin Bennett (Sheriff) <Martin.Bennett@cookcountyil.gov>

Sent: June 23, 2020 3:22:00 PM CDT
Received: June 23, 2020 3:22:32 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: kyara.lee@cookcountyil.gov, Kyara Lee (Sheriff) <Kyara.Lee@cookcountyil.gov>
Sent: June 23, 2020 3:22:00 PM CDT
Received: June 23, 2020 3:22:52 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

To:	Martin Bennett (Sheriff)
Sent:	June 23, 2020 3:22:00 PM CDT
Received:	June 23, 2020 3:22:33 PM CDT

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: michael.gercone@cookcountyil.gov, Michael Gercone (Sheriff) <Michael.Gercone@cookcountyil.gov>

Sent: June 23, 2020 3:22:11 PM CDT
Received: June 23, 2020 3:23:25 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: sajid.haidari@cookcountyil.gov, Sajid Haidari (Sheriff) <Sajid.Haidari@cookcountyil.gov>

Sent: June 23, 2020 3:22:13 PM CDT
Received: June 23, 2020 3:23:50 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: rlobacz@cookcountygov.com, Robert Lobacz (Sheriff) <Robert.Lobacz@cookcountyil.gov>

Sent: June 23, 2020 3:22:32 PM CDT
Received: June 23, 2020 3:22:51 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: tarra.danielsdavis@cookcountyil.gov, Tarra Daniels-Davis (Sheriff) <Tarra.Daniels-Davis@cookcountyil.gov>

Sent: June 23, 2020 3:22:32 PM CDT
Received: June 23, 2020 3:23:11 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: keith.morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: June 23, 2020 3:22:32 PM CDT
Received: June 23, 2020 3:23:17 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: christina.graf@cookcountyil.gov, Christina Graf (Sheriff) <Christina.Graf@cookcountyil.gov>

Sent: June 23, 2020 3:22:32 PM CDT
Received: June 23, 2020 3:23:00 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: henry.hemphill@cookcountyil.gov, Henry Hemphill (Sheriff) <Henry.Hemphill@cookcountyil.gov>

Sent: June 23, 2020 3:22:32 PM CDT
Received: June 23, 2020 3:23:03 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: phillip.mackey@cookcountyil.gov, Phillip Mackey (Sheriff) <Phillip.Mackey@cookcountyil.gov>

Sent: June 23, 2020 3:22:36 PM CDT
Received: June 23, 2020 3:23:33 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: nathan.camer@cookcountyil.gov, Nathan Camer (Sheriff) <Nathan.Camer@cookcountyil.gov>

Sent: June 23, 2020 3:22:36 PM CDT
Received: June 23, 2020 3:24:32 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: joseph.bellettiere@cookcountyil.gov, Joseph Bellettiere (Sheriff) <Joseph.Bellettiere@cookcountyil.gov>

Sent: June 23, 2020 3:22:36 PM CDT
Received: June 23, 2020 3:23:43 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: eroedel@cookcountygov.com, Erik Roedel (Sheriff) <Erik.Roedel@cookcountyil.gov>

Sent: June 23, 2020 3:22:36 PM CDT
Received: June 23, 2020 3:24:32 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: james.minor@cookcountyil.gov, James Minor (Sheriff) <James.Minor@cookcountyil.gov>

Sent: June 23, 2020 3:22:36 PM CDT
Received: June 23, 2020 3:24:27 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: tstajura@cookcountygov.com, Theodore Stajura (Sheriff) <Theodore.Stajura@cookcountyil.gov>

Sent: June 23, 2020 3:22:36 PM CDT
Received: June 23, 2020 3:23:55 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: kendall.evans@cookcountyil.gov, Kendall Evans (Sheriff) <Kendall.Evans@cookcountyil.gov>

Sent: June 23, 2020 3:22:36 PM CDT
Received: June 23, 2020 3:24:19 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: david.cammack@cookcountyil.gov, David Cammack (Sheriff) <David.Cammack@cookcountyil.gov>

Sent: June 23, 2020 3:22:36 PM CDT
Received: June 23, 2020 3:24:15 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: amolina@cookcountygov.com, Adrian Molina (Sheriff) <Adrian.Molina@cookcountyil.gov>

Sent: June 23, 2020 3:22:36 PM CDT
Received: June 23, 2020 3:24:23 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

To: Nathan Camer (Sheriff)
Sent: June 23, 2020 3:22:36 PM CDT
Received: June 23, 2020 3:24:32 PM CDT

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

To: James Minor (Sheriff)
Sent: June 23, 2020 3:22:36 PM CDT
Received: June 23, 2020 3:24:27 PM CDT

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: patrick.dwyer@cookcountyil.gov, Patrick Dwyer (Sheriff) <Patrick.Dwyer@cookcountyil.gov>

Sent: June 23, 2020 3:22:41 PM CDT
Received: June 23, 2020 3:24:34 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: fulvio.compagnone@cookcountyil.gov, Fulvio Compagnone (Sheriff) <Fulvio.Compagnone@cookcountyil.gov>

Sent: June 23, 2020 3:22:41 PM CDT
Received: June 23, 2020 3:24:34 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

To:	Fulvio Compagnone (Sheriff)
Sent:	June 23, 2020 3:22:41 PM CDT
Received:	June 23, 2020 3:24:34 PM CDT

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: terrence.doran@cookcountyil.gov, Terrence Doran (Sheriff) <Terrence.Doran@cookcountyil.gov>

Sent: June 23, 2020 3:22:42 PM CDT
Received: June 23, 2020 3:25:16 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: myron.weres@cookcountyil.gov, Myron Weres (Sheriff) <Myron.Weres@cookcountyil.gov>

Sent: June 23, 2020 3:22:42 PM CDT
Received: June 23, 2020 3:25:02 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: brian.staudt@cookcountyil.gov, Brian Staudt (Sheriff) <Brian.Staudt@cookcountyil.gov>

Sent: June 23, 2020 3:22:56 PM CDT
Received: June 23, 2020 3:25:00 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: mweres@cookcountygov.com, Myron Weres (Sheriff) <Myron.Weres@cookcountyil.gov>

Sent: June 23, 2020 3:22:56 PM CDT
Received: June 23, 2020 3:24:51 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: ycollins@cookcountygov.com, Yolanda Collins-Watson (Sheriff) <Yolanda.Collins-Watson@cookcountyil.gov>

Sent: June 23, 2020 3:23:10 PM CDT
Received: June 23, 2020 3:25:40 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: timothy.odonnell@cookcountyil.gov, Timothy O'Donnell (Sheriff) <Timothy.Odonnell@cookcountyil.gov>

Sent: June 23, 2020 3:23:10 PM CDT
Received: June 23, 2020 3:25:42 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: brian.white@cookcountyil.gov, Brian White (Sheriff) <Brian.White@cookcountyil.gov>

Sent: June 23, 2020 3:23:10 PM CDT
Received: June 23, 2020 3:25:38 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

To:	Timothy O'Donnell (Sheriff)
Sent:	June 23, 2020 3:23:10 PM CDT
Received:	June 23, 2020 3:25:43 PM CDT

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Phillip.lapuma@cookcountyil.gov, Philip Lapuma (Sheriff) <Philip.Lapuma@cookcountyil.gov>

Sent: June 23, 2020 3:23:19 PM CDT
Received: June 23, 2020 3:26:21 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: jennifer.bordoshuk@cookcountyil.gov, Jennifer Bordoshuk (Sheriff) <Jennifer.Bordoshuk@cookcountyil.gov>

Sent: June 23, 2020 3:23:19 PM CDT
Received: June 23, 2020 3:26:45 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: philip.koenig@cookcountyil.gov, Philip Koenig (Sheriff) <Philip.Koenig@cookcountyil.gov>

Sent: June 23, 2020 3:23:19 PM CDT
Received: June 23, 2020 3:25:53 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Clarance.Hummel@CookCountyIl.Gov, Clarance Hummel (Sheriff) <Clarance.Hummel@cookcountyil.gov>

Sent: June 23, 2020 3:23:19 PM CDT
Received: June 23, 2020 3:27:20 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: philip.fraticola@cookcountyil.gov, Philip Fraticola (Sheriff) <Philip.Fraticola@cookcountyil.gov>

Sent: June 23, 2020 3:23:19 PM CDT
Received: June 23, 2020 3:26:16 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: daniel.redican@cookcountyil.gov, Daniel Redican (Sheriff) <Daniel.Redican@cookcountyil.gov>

Sent: June 23, 2020 3:23:19 PM CDT
Received: June 23, 2020 3:26:32 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: jaunesh.carpenter@cookcountyil.gov, Jaunesh Contreras (Sheriff) <Jaunesh.Contreras@cookcountyil.gov>

Sent: June 23, 2020 3:23:19 PM CDT
Received: June 23, 2020 3:25:58 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Joseph.nicholas@cookcountyil.gov, Joseph Nicholas (Sheriff) <Joseph.Nicholas@cookcountyil.gov>

Sent: June 23, 2020 3:23:19 PM CDT
Received: June 23, 2020 3:27:27 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: marianne.kelly@cookcountyil.gov, Marianne Kelly (Sheriff) <Marianne.Kelly@cookcountyil.gov>

Sent: June 23, 2020 3:23:19 PM CDT
Received: June 23, 2020 3:26:00 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: jasmina.janjic@cookcountyil.gov, Jasmina Janjic (Sheriff) <Jasmina.Janjic@cookcountyil.gov>

Sent: June 23, 2020 3:23:19 PM CDT
Received: June 23, 2020 3:27:20 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: john.merola@cookcountyil.gov, John Merola (Sheriff) <John.Merola@cookcountyil.gov>

Sent: June 23, 2020 3:23:19 PM CDT
Received: June 23, 2020 3:26:41 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Gustavo.jimenezjr@cookcountyil.gov, Gustavo Jimenez (Sheriff) <Gustavo.Jimenez@cookcountyil.gov>

Sent: June 23, 2020 3:23:19 PM CDT
Received: June 23, 2020 3:26:15 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

To:	Marianne Kelly (Sheriff)
Sent:	June 23, 2020 3:23:19 PM CDT
Received:	June 23, 2020 3:26:00 PM CDT

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: ricky.soto@cookcountyil.gov, Ricky Soto (Sheriff) <Ricky.Soto@cookcountyil.gov>

Sent: June 23, 2020 3:23:27 PM CDT
Received: June 23, 2020 3:26:55 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: andre.blue@cookcountyil.gov, Andre Blue (Sheriff) <Andre.Blue@cookcountyil.gov>

Sent: June 23, 2020 3:23:27 PM CDT
Received: June 23, 2020 3:26:54 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: walter.klinger@cookcountyil.gov, Walter Klinger (Sheriff) <Walter.Klinger@cookcountyil.gov>

Sent: June 23, 2020 3:23:32 PM CDT
Received: June 23, 2020 3:24:33 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: antonio.imhof@cookcountyil.gov, Antonio Imhof (Sheriff) <Antonio.Imhof@cookcountyil.gov>

Sent: June 23, 2020 3:23:32 PM CDT
Received: June 23, 2020 3:25:25 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: michelle.kaechele@cookcountyil.gov, Michelle Kaechele (Sheriff) <Michelle.Kaechele@cookcountyil.gov>

Sent: June 23, 2020 3:23:32 PM CDT
Received: June 23, 2020 3:24:43 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Albert.Carter@cookcountyil.gov, Albert Carter (Sheriff) <Albert.Carter@cookcountyil.gov>

Sent: June 23, 2020 3:23:32 PM CDT
Received: June 23, 2020 3:24:55 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: stavone.mcherron@cookcountyil.gov, Stavone McHerron (Sheriff) <Stavone.Mcherron@cookcountyil.gov>

Sent: June 23, 2020 3:23:32 PM CDT
Received: June 23, 2020 3:25:12 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

To:	Walter Klinger (Sheriff)
Sent:	June 23, 2020 3:23:32 PM CDT
Received:	June 23, 2020 3:24:34 PM CDT

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: thomas.goshen@cookcountyil.gov, Thomas Goshen (Sheriff) <Thomas.Goshen@cookcountyil.gov>

Sent: June 23, 2020 3:23:38 PM CDT
Received: June 23, 2020 3:25:59 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Rebecca.DeJesus@cookcountyil.gov, Rebecca Dejesus (Sheriff) <Rebecca.Dejesus@cookcountyil.gov>

Sent: June 23, 2020 3:23:38 PM CDT
Received: June 23, 2020 3:25:37 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Richard.obrien2@cookcountyil.gov, Richard O'Brien (Sheriff) <richard.obrien2@cookcountyil.gov>

Sent: June 23, 2020 3:23:38 PM CDT
Received: June 23, 2020 3:25:54 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: aaron.harris@cookcountyil.gov, Aaron Harris (Sheriff) <Aaron.Harris@cookcountyil.gov>

Sent: June 23, 2020 3:23:38 PM CDT
Received: June 23, 2020 3:26:20 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: christopher.harvey@cookcountyil.gov, Christopher Harvey (Sheriff) <Christopher.Harvey@cookcountyil.gov>

Sent: June 23, 2020 3:23:38 PM CDT
Received: June 23, 2020 3:25:40 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

To: Aaron Harris (Sheriff)
Sent: June 23, 2020 3:23:38 PM CDT
Received: June 23, 2020 3:26:21 PM CDT

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: michael.rowe@cookcountyil.gov, Michael Rowe (Sheriff) <Michael.Rowe@cookcountyil.gov>

Sent: June 23, 2020 3:23:49 PM CDT
Received: June 23, 2020 3:26:40 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: thomas.staples@cookcountyil.gov, Thomas Staples (Sheriff) <Thomas.Staples@cookcountyil.gov>

Sent: June 23, 2020 3:23:49 PM CDT
Received: June 23, 2020 3:26:54 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: katerina.klopas@cookcountyil.gov, Katerina Klopas (Sheriff) <Katerina.Klopas@cookcountyil.gov>

Sent: June 23, 2020 3:23:59 PM CDT
Received: June 23, 2020 3:24:27 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

To:	Katerina Klopas (Sheriff)
Sent:	June 23, 2020 3:23:59 PM CDT
Received:	June 23, 2020 3:24:28 PM CDT

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: debra.clark@cookcountyil.gov, Debra Clark (Sheriff) <Debra.Clark@cookcountyil.gov>

Sent: June 23, 2020 3:24:25 PM CDT
Received: June 23, 2020 3:25:07 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Randall.Pochie@cookcountyil.gov, Randall Pochie (Sheriff) <Randall.Pochie@cookcountyil.gov>

Sent: June 23, 2020 3:24:25 PM CDT
Received: June 23, 2020 3:24:44 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: neal.gaynor@cookcountyil.gov, Neal Gaynor (Sheriff) <Neal.Gaynor@cookcountyil.gov>

Sent: June 23, 2020 3:24:25 PM CDT
Received: June 23, 2020 3:24:58 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: carl.price@cookcountyil.gov, Carl Price (Sheriff) <Carl.Price@cookcountyil.gov>
Sent: June 23, 2020 3:24:25 PM CDT
Received: June 23, 2020 3:25:06 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: agoulos@cookcountygov.com, Anastasios Goulos (Sheriff) <Anastasios.Goulos@cookcountyil.gov>

Sent: June 23, 2020 3:24:29 PM CDT
Received: June 23, 2020 3:25:45 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: anthony.sevening@cookcountyil.gov, Anthony Sevening (Sheriff) <Anthony.Sevening@cookcountyil.gov>

Sent: June 23, 2020 3:24:29 PM CDT
Received: June 23, 2020 3:25:30 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

To: Anastasios Goulos (Sheriff)
Sent: June 23, 2020 3:24:29 PM CDT
Received: June 23, 2020 3:25:45 PM CDT

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: arthur.jackson@cookcountyil.gov, Arthur Jackson (Sheriff) <Arthur.Jackson@cookcountyil.gov>

Sent: June 23, 2020 3:24:52 PM CDT
Received: June 23, 2020 3:25:37 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: juan.claudio@cookcountyil.gov, Juan Claudio (Sheriff) <Juan.Claudio@cookcountyil.gov>

Sent: June 23, 2020 3:24:57 PM CDT
Received: June 23, 2020 3:25:02 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Miguel.Mancha@cookcountyil.gov, Miguel Mancha (Sheriff) <Miguel.Mancha@cookcountyil.gov>

Sent: June 23, 2020 3:24:57 PM CDT
Received: June 23, 2020 3:25:18 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: jazmond.watson@cookcountyil.gov, Jazmond Watson (Sheriff) <Jazmond.Watson@cookcountyil.gov>

Sent: June 23, 2020 3:24:57 PM CDT
Received: June 23, 2020 3:25:08 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: george.winistorfer@cookcountyil.gov, George Winistorfer (Sheriff) <George.Winistorfer@cookcountyil.gov>

Sent: June 23, 2020 3:25:07 PM CDT
Received: June 23, 2020 3:25:25 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: jclaudio@cookcountygov.com, Juan Claudio (Sheriff) <Juan.Claudio@cookcountyil.gov>

Sent: June 23, 2020 3:25:07 PM CDT
Received: June 23, 2020 3:25:25 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: patricia.echols@cookcountyil.gov, Patricia Montgomery-Echols (Sheriff) <Patricia.Montgomery-echols@cookcountyil.gov>

Sent: June 23, 2020 3:25:08 PM CDT
Received: June 23, 2020 3:25:26 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: nicky.nunez@cookcountyil.gov, Nicky Nunez (Sheriff) <Nicky.Nunez@cookcountyil.gov>

Sent: June 23, 2020 3:25:37 PM CDT
Received: June 23, 2020 3:26:04 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: jrosenau@cookcountygov.com, Joseph Rosenau (Sheriff) <Joseph.Rosenau@cookcountyil.gov>

Sent: June 23, 2020 3:25:37 PM CDT
Received: June 23, 2020 3:25:40 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Joseph.Phillips@cookcountyil.gov, Joseph Phillips (Sheriff) <Joseph.Phillips@cookcountyil.gov>

Sent: June 23, 2020 3:25:37 PM CDT
Received: June 23, 2020 3:25:51 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: antoinette.steele@cookcountyil.gov, Antoinette Bradley (Sheriff) <Antoinette.Bradley@cookcountyil.gov>

Sent: June 23, 2020 3:25:49 PM CDT
Received: June 23, 2020 3:26:51 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: ccspdtraining@cookcountygov.com, Sheriff Training (Sheriff) <Sheriff.Training@cookcountyil.gov>

Sent: June 23, 2020 3:25:49 PM CDT
Received: June 23, 2020 3:27:00 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: rogelio.martinez@cookcountyil.gov, Rogelio Martinez (Sheriff) <Rogelio.Martinez@cookcountyil.gov>

Sent: June 23, 2020 3:25:57 PM CDT
Received: June 23, 2020 3:26:05 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: mgoral@cookcountygov.com, Matthew Goral (Sheriff) <Matthew.Goral@cookcountyil.gov>

Sent: June 23, 2020 3:26:07 PM CDT
Received: June 23, 2020 3:26:58 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Marcus.jackson@cookcountyil.gov, Marcus Jackson (Sheriff) <Marcus.Jackson@cookcountyil.gov>

Sent: June 23, 2020 3:26:28 PM CDT
Received: June 23, 2020 3:26:45 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Ryan.Huber@cookcountyil.gov, Ryan Huber (Sheriff) <Ryan.Huber@cookcountyil.gov>

Sent: June 23, 2020 3:26:36 PM CDT
Received: June 23, 2020 3:27:43 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Erica.pepper@cookcountyil.gov, Erica Pepper (Sheriff) <Erica.Pepper@cookcountyil.gov>

Sent: June 23, 2020 3:26:56 PM CDT
Received: June 23, 2020 3:27:29 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: Ron.avelino@cookcountyil.gov, Ron Avelino (Sheriff) <Ron.Avelino@cookcountyil.gov>

Sent: June 23, 2020 3:26:56 PM CDT
Received: June 23, 2020 3:27:54 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: trohl@cookcountygov.com, Todd Rohl (Sheriff) <Todd.Rohl@cookcountyil.gov>

Sent: June 23, 2020 3:27:14 PM CDT
Received: June 23, 2020 3:27:32 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack

From: PoliceOne Roll Call <newsletter@policeone.com>
To: mgoldsmith@cookcountygov.com, Michael Goldsmith (Sheriff) <Michael.Goldsmith@cookcountyil.gov>

Sent: June 23, 2020 3:27:14 PM CDT
Received: June 23, 2020 3:27:59 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 23, 2020 | View as webpage

TOP STORIES

Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes

Minn. police union says it's been 'scapegoated' after Floyd death

Police investigate 3rd shooting near Seattle's 'occupied' protest zone

Democrats demand more changes, greater accountability in GOP police bill

'BlueLeaks' exposes files from hundreds of US police departments

Bystander helps save Pa. police officer following fiery crash

Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

Learn more

FEATURED CONTENT

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic easier.

Watch it on-demand

Your In-Car Clutter May Prevent Airbags From Saving Your Life

Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out the link below for more info.

Learn how

OTHER HIGHLIGHTS

Are you ready to testify?

By Val Van Brocklin

Tips on being an effective witness

Preparing for a court appearance

By Gordon Graham

Follow these steps to ensure you are adequately prepped

SPONSORED CONTENT

Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with performance evaluations. Download this white paper to learn how to avoid four common mistakes. Learn more.

FEATURED EDUCATION

Advance Your Career, at Your Own Pace

Claim your training credits.

FEATURED EDUCATION

University of Cincinnati Online

100% online bachelor's & master's in Criminal Justice programs. Learn more!

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

FW: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

From: Jonathan Springborn (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=32F2A0A9AA124C638CA1784E3422B464-JONATHAN SP>
To: Keith Morrison (Keith.Morrison@cookcountyil.gov) <Keith.Morrison@cookcountyil.gov>, Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent: June 23, 2020 4:27:34 PM CDT
Received: June 23, 2020 4:27:00 PM CDT

FYI,

You may want to check out this alert and URL.

Data breach affected: Illinois Crime Reporting and Information - Metro East

https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>
Sent: Tuesday, June 23, 2020 11:04 AM
To: Michael Aliperti <Michael.Aliperti@cisecurity.org>; Ben Spear <Ben.Spear@cisecurity.org>
Subject: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

TLP: AMBER

TO: All MS-ISAC Members and Partners

DATE: June 23, 2020

SUBJECT: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach

On June 19, 2020, a Twitter account announced the leak of 10 years of data from police departments, fusion centers, and other law enforcement-related entities currently being tracked on social media as #BlueLeaks. According to the National Fusion Center Association (NFCA), the leak is the result of a compromise at a third party web hosting company, Netsential.

The Twitter account is associated with Distributed Denial of Secrets (DDOS), a collective known for posting leaked or exfiltrated data. The post included a link to a Dark Web location hosting 269GB of files and emails including bulletins, advisories, and guides.

Upon receiving notification of this data breach, the MS-ISAC has confirmed the existence of the dataset and is currently working to analyze the specific contents of the data along with our federal, state, and local

partners. At this time, some MS-ISAC products and correspondence have been identified in the leaked data due to the nature of our relationship with fusion centers and law enforcement entities. It is likely that cyber threat actors will utilize MS-ISAC information and/or other portions of the data dump to create tailored phishing campaigns or conduct other malicious cyber activity.

Recommendations:

- Be vigilant for new waves of phishing campaigns spoofing emails or products.
- Implement Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-Based Message Authentication Reporting and Conformance (DMARC), which will assist in ensuring that senders are unable to spoof your email domain. For assistance in implementing these controls, see the Global Cyber Alliance's DMARC Guide https://dmarcguide.globalcyberalliance.org/#/.
- Ensure anti-virus software is up to date.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

The MS-ISAC continues to monitor this situation closely and will release further information as appropriate.

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722



TLP: AMBER

Limited Disclosure, restricted to participants' organizations. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.

RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

From: Patrick Kelly (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=873FFD393E8C44B79E707E6A1056650A-PATRICK KEL>
To: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent: June 23, 2020 4:35:19 PM CDT
Received: June 23, 2020 4:35:00 PM CDT

Wow…that is crazy. Not good at all.

From: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 4:28 PM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: FW: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER
Importance: High

FYI,

You may want to check out this alert and URL.

Data breach affected: Illinois Crime Reporting and Information - Metro East

https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>
Sent: Tuesday, June 23, 2020 11:04 AM
To: Michael Aliperti <Michael.Aliperti@cisecurity.org>; Ben Spear <Ben.Spear@cisecurity.org>
Subject: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

TLP: AMBER

TO: All MS-ISAC Members and Partners

DATE: June 23, 2020

SUBJECT: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach

On June 19, 2020, a Twitter account announced the leak of 10 years of data from police departments, fusion centers, and other law enforcement-related entities currently being tracked on social media as #BlueLeaks. According to the National Fusion Center Association (NFCA), the leak is the result of a compromise at a third party web hosting company, Netsential.

The Twitter account is associated with Distributed Denial of Secrets (DDOS), a collective known for posting leaked or exfiltrated data. The post included a link to a Dark Web location hosting 269GB of files and emails including bulletins, advisories, and guides.

Upon receiving notification of this data breach, the MS-ISAC has confirmed the existence of the dataset and is currently working to analyze the specific contents of the data along with our federal, state, and local partners. At this time, some MS-ISAC products and correspondence have been identified in the leaked data due to the nature of our relationship with fusion centers and law enforcement entities. It is likely that cyber threat actors will utilize MS-ISAC information and/or other portions of the data dump to create tailored phishing campaigns or conduct other malicious cyber activity.

Recommendations:

- Be vigilant for new waves of phishing campaigns spoofing emails or products.
- Implement Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-Based Message Authentication Reporting and Conformance (DMARC), which will assist in ensuring that senders are unable to spoof your email domain. For assistance in implementing these controls, see the Global Cyber Alliance's DMARC Guide https://dmarcguide.globalcyberalliance.org/#/.
- Ensure anti-virus software is up to date.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

The MS-ISAC continues to monitor this situation closely and will release further information as appropriate.

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722



TLP: AMBER

Limited Disclosure, restricted to participants' organizations. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.

RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

From: Jonathan Springborn (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=32F2A0A9AA124C638CA1784E3422B464-JONATHAN SP>
To: Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent: June 23, 2020 4:38:23 PM CDT
Received: June 23, 2020 4:38:00 PM CDT

Agreed.

I found these entities close to us that were affected:

Wisconsin Statewide Intelligence Center

FBI National Academy Association Michigan Chapter

Iowa Law Enforcement Academy

Iowa Fusion Center

Missouri Information Analysis Center

I don't know if we interact much if at all, but they are close by.

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 4:35 PM
To: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

Wow…that is crazy. Not good at all.

From: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 4:28 PM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: FW: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER
Importance: High

FYI,

You may want to check out this alert and URL.

Data breach affected: Illinois Crime Reporting and Information - Metro East

https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>
Sent: Tuesday, June 23, 2020 11:04 AM
To: Michael Aliperti <Michael.Aliperti@cisecurity.org>; Ben Spear <Ben.Spear@cisecurity.org>
Subject: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

TLP: AMBER

TO: All MS-ISAC Members and Partners

DATE: June 23, 2020

SUBJECT: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach

On June 19, 2020, a Twitter account announced the leak of 10 years of data from police departments, fusion centers, and other law enforcement-related entities currently being tracked on social media as #BlueLeaks. According to the National Fusion Center Association (NFCA), the leak is the result of a compromise at a third party web hosting company, Netsential.

The Twitter account is associated with Distributed Denial of Secrets (DDOS), a collective known for posting leaked or exfiltrated data. The post included a link to a Dark Web location hosting 269GB of files and emails including bulletins, advisories, and guides.

Upon receiving notification of this data breach, the MS-ISAC has confirmed the existence of the dataset and is currently working to analyze the specific contents of the data along with our federal, state, and local partners. At this time, some MS-ISAC products and correspondence have been identified in the leaked data due to the nature of our relationship with fusion centers and law enforcement entities. It is likely that cyber threat actors will utilize MS-ISAC information and/or other portions of the data dump to create tailored phishing campaigns or conduct other malicious cyber activity.

Recommendations:

- Be vigilant for new waves of phishing campaigns spoofing emails or products.
- Implement Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-Based Message Authentication Reporting and Conformance (DMARC), which will assist in ensuring that senders are unable to spoof your email domain. For assistance in implementing these controls, see the Global Cyber Alliance's DMARC Guide https://dmarcguide.globalcyberalliance.org/#/.
- Ensure anti-virus software is up to date.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

The MS-ISAC continues to monitor this situation closely and will release further information as appropriate.

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722



TLP: AMBER

Limited Disclosure, restricted to participants' organizations. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.

RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

To: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent: June 23, 2020 4:42:33 PM CDT
Received: June 23, 2020 4:42:21 PM CDT

Yeah. I saw Infragard (San Francisco) is one of them.

From: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 4:38 PM
To: Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

Agreed.

I found these entities close to us that were affected:

Wisconsin Statewide Intelligence Center
FBI National Academy Association Michigan Chapter
Iowa Law Enforcement Academy
Iowa Fusion Center
Missouri Information Analysis Center

I don't know if we interact much if at all, but they are close by.

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 4:35 PM
To: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

Wow…that is crazy. Not good at all.

From: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 4:28 PM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: FW: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data

Breach - TLP: AMBER
Importance: High

FYI,

You may want to check out this alert and URL.

Data breach affected: Illinois Crime Reporting and Information - Metro East

https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>
Sent: Tuesday, June 23, 2020 11:04 AM
To: Michael Aliperti <Michael.Aliperti@cisecurity.org>; Ben Spear <Ben.Spear@cisecurity.org>
Subject: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

TLP: AMBER

TO: All MS-ISAC Members and Partners

DATE: June 23, 2020

SUBJECT: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach

On June 19, 2020, a Twitter account announced the leak of 10 years of data from police departments, fusion centers, and other law enforcement-related entities currently being tracked on social media as #BlueLeaks. According to the National Fusion Center Association (NFCA), the leak is the result of a compromise at a third party web hosting company, Netsential.

The Twitter account is associated with Distributed Denial of Secrets (DDOS), a collective known for posting leaked or exfiltrated data. The post included a link to a Dark Web location hosting 269GB of files and emails including bulletins, advisories, and guides.

Upon receiving notification of this data breach, the MS-ISAC has confirmed the existence of the dataset and is currently working to analyze the specific contents of the data along with our federal, state, and local partners. At this time, some MS-ISAC products and correspondence have been identified in the leaked data due to the nature of our relationship with fusion centers and law enforcement entities. It is likely that cyber threat actors will utilize MS-ISAC information and/or other portions of the data dump to create tailored phishing campaigns or conduct other malicious cyber activity.

Recommendations:

- Be vigilant for new waves of phishing campaigns spoofing emails or products.
- Implement Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-Based Message Authentication Reporting and Conformance (DMARC), which will assist in ensuring

that senders are unable to spoof your email domain. For assistance in implementing these controls, see the Global Cyber Alliance's DMARC Guide https://dmarcguide.globalcyberalliance.org/#/.
- Ensure anti-virus software is up to date.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

The MS-ISAC continues to monitor this situation closely and will release further information as appropriate.

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722



TLP: AMBER

Limited Disclosure, restricted to participants' organizations. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.

RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

To: Jonathan Springborn (Sheriff), Keith Morrison (Sheriff), Christopher Moore (Sheriff)
Sent: June 23, 2020 4:42:33 PM CDT
Received: June 23, 2020 4:42:21 PM CDT

Man Saves Officer from Wrecked Patrol Car

From: Police On Target <PoliceOnTarget@bobitenews.com>
To: edward.lewandowski@cookcountyil.gov, Edward Lewandowski (Sheriff) <Edward.Lewandowski@cookcountyil.gov>
Sent: June 23, 2020 5:23:28 PM CDT
Received: June 23, 2020 5:23:31 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Jun 23, 2020 View online version

ONTARGET TUESDAY

Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

READ MORE

Hackers Steals Massive Trove of Police Files, Post Them Online

DDoSecrets said the BlueLeaks archive indexes “ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources,” and that “among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more.”

READ MORE

Florida Officers Lured Into Ambush Attack at Call for Service

Several officers with the Tampa (LF) Police Department were reportedly ambushed early Saturday morning while responding to a call for service.

READ MORE

Maryland Officer Wounded by Gunfire Released from Hospital

An officer with the Baltimore Police Department who was shot earlier this month while he tried to disperse a large crowd that had gathered to protest the in-custody death of George Floyd in Minneapolis has been released from the hospital.

READ MORE

Responding to Domestic Disturbances

A domestic disturbance call can involve anything from

a verbal dispute to a homicide. So we all need reminders of the danger of domestic disputes and ensure officers are taking all precautions.

READ MORE

Massachusetts Officer Injured in Attack During Interview at Police Station

An officer with the Southborough (MA) Police Department was injured after he was reportedly assaulted with a weapon inside a police station on Monday night.

READ MORE

Oregon Officer Saves Infant from Burning Home

An officer with the Astoria (OR) Police Department is being heralded as a hero for his quick actions late last week that are now only becoming public knowledge.

READ MORE

Texas Officer Shot in Arm Following Vehicle and Foot Pursuit

An officer with the Watauga (TX) Police Department was shot in the arm by a suspect who led police on a vehicle chase, bailed out of the car and ran away, briefly eluding officers.

READ MORE

Hybrids Ready for Patrol

Police vehicles with hybrid gas-electric engines will save law enforcement agencies money and cut

emissions. More importantly, they can do the job.

READ MORE

FREE WHITEPAPERS

- SPECIAL REPORT: Drug Enforcement, Protection & Testing
- Police and the Coronavirus Pandemic
- SPECIAL REPORT: Fleet Management & Upfitting
- Special Report: Preventing & Preparing for Workplace Attacks
- Best Practices for Setting Up and Implementing a First Responder Network
- Special Report: Software & Mobile Apps
- Special Report: Ballistic Protection
- The Top 5 Emerging Technologies Police Agencies Can't Do Without
- How Technology Mitigates Threats at Large-Scale Events
- Special Report: Critical Incident Response
- Special Report: Upfitting & Fleet Management

POLICE MAGAZINE

You are currently subscribed as edward.lewandowski@cookcountyil.gov. Manage your email preferences.

Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Man Saves Officer from Wrecked Patrol Car

To:	Edward Lewandowski (Sheriff)
Sent:	June 23, 2020 5:23:28 PM CDT
Received:	June 23, 2020 5:23:31 PM CDT

Man Saves Officer from Wrecked Patrol Car

From: Police On Target <PoliceOnTarget@bobitenews.com>
To: larry.schurig@cookcountyil.gov, Larry Schurig (Sheriff) <Larry.Schurig@cookcountyil.gov>
Sent: June 23, 2020 5:24:40 PM CDT
Received: June 23, 2020 5:24:59 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Jun 23, 2020 View online version

ONTARGET TUESDAY

Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

READ MORE

Hackers Steals Massive Trove of Police Files, Post Them Online

DDoSecrets said the BlueLeaks archive indexes “ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources,” and that “among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more.”

READ MORE

Florida Officers Lured Into Ambush Attack at Call for Service

Several officers with the Tampa (LF) Police Department were reportedly ambushed early Saturday morning while responding to a call for service.

READ MORE

Maryland Officer Wounded by Gunfire Released from Hospital

An officer with the Baltimore Police Department who was shot earlier this month while he tried to disperse a large crowd that had gathered to protest the in-custody death of George Floyd in Minneapolis has been released from the hospital.

READ MORE

Responding to Domestic Disturbances

A domestic disturbance call can involve anything from

a verbal dispute to a homicide. So we all need reminders of the danger of domestic disputes and ensure officers are taking all precautions.

READ MORE

Massachusetts Officer Injured in Attack During Interview at Police Station

An officer with the Southborough (MA) Police Department was injured after he was reportedly assaulted with a weapon inside a police station on Monday night.

READ MORE

Oregon Officer Saves Infant from Burning Home

An officer with the Astoria (OR) Police Department is being heralded as a hero for his quick actions late last week that are now only becoming public knowledge.

READ MORE

Texas Officer Shot in Arm Following Vehicle and Foot Pursuit

An officer with the Watauga (TX) Police Department was shot in the arm by a suspect who led police on a vehicle chase, bailed out of the car and ran away, briefly eluding officers.

READ MORE

Hybrids Ready for Patrol

Police vehicles with hybrid gas-electric engines will save law enforcement agencies money and cut

emissions. More importantly, they can do the job.

READ MORE

FREE WHITEPAPERS

- SPECIAL REPORT: Drug Enforcement, Protection & Testing
- Police and the Coronavirus Pandemic
- SPECIAL REPORT: Fleet Management & Upfitting
- Special Report: Preventing & Preparing for Workplace Attacks
- Best Practices for Setting Up and Implementing a First Responder Network
- Special Report: Software & Mobile Apps
- Special Report: Ballistic Protection
- The Top 5 Emerging Technologies Police Agencies Can't Do Without
- How Technology Mitigates Threats at Large-Scale Events
- Special Report: Critical Incident Response
- Special Report: Upfitting & Fleet Management

POLICE MAGAZINE

You are currently subscribed as larry.schurig@cookcountyil.gov. Manage your email preferences.

Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Man Saves Officer from Wrecked Patrol Car

From: Police On Target <PoliceOnTarget@bobitenews.com>
To: david.griffin@cookcountyil.gov, David Griffin (Sheriff) <David.Griffin@cookcountyil.gov>
Sent: June 23, 2020 5:25:10 PM CDT
Received: June 23, 2020 5:25:13 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Jun 23, 2020 View online version

ONTARGET TUESDAY

Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

READ MORE

Hackers Steals Massive Trove of Police Files, Post Them Online

DDoSecrets said the BlueLeaks archive indexes “ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources,” and that “among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more.”

READ MORE

Florida Officers Lured Into Ambush Attack at Call for Service

Several officers with the Tampa (LF) Police Department were reportedly ambushed early Saturday morning while responding to a call for service.

READ MORE

Maryland Officer Wounded by Gunfire Released from Hospital

An officer with the Baltimore Police Department who was shot earlier this month while he tried to disperse a large crowd that had gathered to protest the in-custody death of George Floyd in Minneapolis has been released from the hospital.

READ MORE

Responding to Domestic Disturbances

A domestic disturbance call can involve anything from

a verbal dispute to a homicide. So we all need reminders of the danger of domestic disputes and ensure officers are taking all precautions.

READ MORE

Massachusetts Officer Injured in Attack During Interview at Police Station

An officer with the Southborough (MA) Police Department was injured after he was reportedly assaulted with a weapon inside a police station on Monday night.

READ MORE

Oregon Officer Saves Infant from Burning Home

An officer with the Astoria (OR) Police Department is being heralded as a hero for his quick actions late last week that are now only becoming public knowledge.

READ MORE

Texas Officer Shot in Arm Following Vehicle and Foot Pursuit

An officer with the Watauga (TX) Police Department was shot in the arm by a suspect who led police on a vehicle chase, bailed out of the car and ran away, briefly eluding officers.

READ MORE

Hybrids Ready for Patrol

Police vehicles with hybrid gas-electric engines will save law enforcement agencies money and cut

emissions. More importantly, they can do the job.

READ MORE

FREE WHITEPAPERS

- SPECIAL REPORT: Drug Enforcement, Protection & Testing
- Police and the Coronavirus Pandemic
- SPECIAL REPORT: Fleet Management & Upfitting
- Special Report: Preventing & Preparing for Workplace Attacks
- Best Practices for Setting Up and Implementing a First Responder Network
- Special Report: Software & Mobile Apps
- Special Report: Ballistic Protection
- The Top 5 Emerging Technologies Police Agencies Can't Do Without
- How Technology Mitigates Threats at Large-Scale Events
- Special Report: Critical Incident Response
- Special Report: Upfitting & Fleet Management

POLICE MAGAZINE

You are currently subscribed as david.griffin@cookcountyil.gov. Manage your email preferences.

Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Man Saves Officer from Wrecked Patrol Car

To:	David Griffin (Sheriff)
Sent:	June 23, 2020 5:25:10 PM CDT
Received:	June 23, 2020 5:25:13 PM CDT

Man Saves Officer from Wrecked Patrol Car

From: Police On Target <PoliceOnTarget@bobitenews.com>
To: brian.white@cookcountyil.gov, Brian White (Sheriff) <Brian.White@cookcountyil.gov>
Sent: June 23, 2020 5:25:30 PM CDT
Received: June 23, 2020 5:25:38 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Jun 23, 2020 View online version

ONTARGET TUESDAY

Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

READ MORE

Hackers Steals Massive Trove of Police Files, Post Them Online

DDoSecrets said the BlueLeaks archive indexes “ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources,” and that “among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more.”

READ MORE

Florida Officers Lured Into Ambush Attack at Call for Service

Several officers with the Tampa (LF) Police Department were reportedly ambushed early Saturday morning while responding to a call for service.

READ MORE

Maryland Officer Wounded by Gunfire Released from Hospital

An officer with the Baltimore Police Department who was shot earlier this month while he tried to disperse a large crowd that had gathered to protest the in-custody death of George Floyd in Minneapolis has been released from the hospital.

READ MORE

Responding to Domestic Disturbances

A domestic disturbance call can involve anything from

a verbal dispute to a homicide. So we all need reminders of the danger of domestic disputes and ensure officers are taking all precautions.

READ MORE

Massachusetts Officer Injured in Attack During Interview at Police Station

An officer with the Southborough (MA) Police Department was injured after he was reportedly assaulted with a weapon inside a police station on Monday night.

READ MORE

Oregon Officer Saves Infant from Burning Home

An officer with the Astoria (OR) Police Department is being heralded as a hero for his quick actions late last week that are now only becoming public knowledge.

READ MORE

Texas Officer Shot in Arm Following Vehicle and Foot Pursuit

An officer with the Watauga (TX) Police Department was shot in the arm by a suspect who led police on a vehicle chase, bailed out of the car and ran away, briefly eluding officers.

READ MORE

Hybrids Ready for Patrol

Police vehicles with hybrid gas-electric engines will save law enforcement agencies money and cut

emissions. More importantly, they can do the job.

READ MORE

FREE WHITEPAPERS

- SPECIAL REPORT: Drug Enforcement, Protection & Testing
- Police and the Coronavirus Pandemic
- SPECIAL REPORT: Fleet Management & Upfitting
- Special Report: Preventing & Preparing for Workplace Attacks
- Best Practices for Setting Up and Implementing a First Responder Network
- Special Report: Software & Mobile Apps
- Special Report: Ballistic Protection
- The Top 5 Emerging Technologies Police Agencies Can't Do Without
- How Technology Mitigates Threats at Large-Scale Events
- Special Report: Critical Incident Response
- Special Report: Upfitting & Fleet Management

POLICE MAGAZINE

You are currently subscribed as brian.white@cookcountyil.gov. Manage your email preferences.

Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

From:	A BUNTINAS <lietuvis_75@hotmail.com>
To:	Arunas Buntinas <arunas.buntinas2@cookcountyil.gov>, Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov>
Sent:	June 23, 2020 5:48:16 PM CDT
Received:	June 23, 2020 5:48:24 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Group Posts 269 GB of Data Stolen from US Law Enforcement Databases

(June 22, 2020)

A group calling itself Distributed Denial of Secrets has posted 269 gigabytes of police data online. According to a memo from the National Fusion Center Association obtained by Brian Krebs, the data were taken from state owned and operated law enforcement fusion centers, which serve to coordinate communications between state, local, federal, tribal, territorial, private law enforcement partners. The memo notes that “Preliminary analysis of the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centers, law enforcement, and other government agencies across the United States, was the source of the compromise.”

Read more in:
- **krebsonsecurity.com**: ‘BlueLeaks’ Exposes Files from Hundreds of Police Departments
- **arstechnica.com**: Millions of documents from >200 US police agencies published in “BlueLeaks” trove
- **www.wired.com**: Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents
- **www.zdnet.com**: BlueLeaks: Data from 200 US police departments & fusion centers published online
- **www.cyberscoop.com**: 'Distributed Denial of Secrets' publishes 'Blue Leaks,' a trove of law enforcement records
- **www.vice.com**: ‘BlueLeaks’: Group Releases 270GB of Sensitive Police Documents

Data Stolen from US Law Enforcement Databases

From:	Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov>
To:	Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov>, Marlon Parks (Sheriff) <Marlon.Parks@cookcountyil.gov>, Brian White (Sheriff) <Brian.White@cookcountyil.gov>
Sent:	June 23, 2020 5:49:35 PM CDT
Received:	June 23, 2020 5:49:37 PM CDT

Group Posts 269 GB of Data Stolen from US Law Enforcement Databases

(June 22, 2020)

A group calling itself Distributed Denial of Secrets has posted 269 gigabytes of police data online. According to a memo from the National Fusion Center Association obtained by Brian Krebs, the data were taken from state owned and operated law enforcement fusion centers, which serve to coordinate communications between state, local, federal, tribal, territorial, private law enforcement partners. The memo notes that “Preliminary analysis of the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centers, law enforcement, and other government agencies across the United States, was the source of the compromise.”

Read more in:
- **krebsonsecurity.com**: ‘BlueLeaks’ Exposes Files from Hundreds of Police Departments
- **arstechnica.com**: Millions of documents from >200 US police agencies published in “BlueLeaks” trove
- **www.wired.com**: Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents
- **www.zdnet.com**: BlueLeaks: Data from 200 US police departments & fusion centers published online
- **www.cyberscoop.com**: 'Distributed Denial of Secrets' publishes 'Blue Leaks,' a trove of law enforcement records
- **www.vice.com**: ‘BlueLeaks’: Group Releases 270GB of Sensitive Police Documents

Sent from my iPhone

Re: Data Stolen from US Law Enforcement Databases

From:	Leo.Schmitz@cookcountyil.gov
To:	Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov>
Cc:	Marlon Parks (Sheriff) <Marlon.Parks@cookcountyil.gov>, Brian White (Sheriff) <Brian.White@cookcountyil.gov>
Sent:	June 23, 2020 7:36:19 PM CDT
Received:	June 23, 2020 7:36:19 PM CDT

Did they get any of our info?

Leo P. Schmitz
Chief of Public Safety
Cook County Sheriffs Department

Sent from my iPhone

E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

> On Jun 23, 2020, at 5:49 PM, Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov> wrote:

Group Posts 269 GB of Data Stolen from US Law Enforcement Databases

(June 22, 2020)

A group calling itself Distributed Denial of Secrets has posted 269 gigabytes of police data online. According to a memo from the National Fusion Center Association obtained by Brian Krebs, the data were taken from state owned and operated law enforcement fusion centers, which serve to coordinate communications between state, local, federal, tribal, territorial, private law enforcement partners. The memo notes that "Preliminary analysis of the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centers, law enforcement, and other government agencies across the United States, was the source of the compromise."

Read more in:
- **krebsonsecurity.com**: 'BlueLeaks' Exposes Files from Hundreds of Police Departments
- **arstechnica.com**: Millions of documents from >200 US police agencies published in "BlueLeaks" trove
- **www.wired.com**: Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents
- **www.zdnet.com**: BlueLeaks: Data from 200 US police departments & fusion centers published online
- **www.cyberscoop.com**: 'Distributed Denial of Secrets' publishes 'Blue Leaks,' a trove of law enforcement records
- **www.vice.com**: 'BlueLeaks': Group Releases 270GB of Sensitive Police Documents

Sent from my iPhone

Re: Data Stolen from US Law Enforcement Databases

From:	Leo Schmitz (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D9CD12213A744B67BF85F400559CE4A7-LEO SCHMITZ>
To:	Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov>
Cc:	Marlon Parks (Sheriff) <Marlon.Parks@cookcountyil.gov>, Brian White (Sheriff) <Brian.White@cookcountyil.gov>
Sent:	June 23, 2020 7:36:19 PM CDT
Received:	June 23, 2020 7:36:20 PM CDT

Did they get any of our info?

Leo P. Schmitz
Chief of Public Safety
Cook County Sheriffs Department

Sent from my iPhone

E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

On Jun 23, 2020, at 5:49 PM, Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov> wrote:

Group Posts 269 GB of Data Stolen from US Law Enforcement Databases

(June 22, 2020)

A group calling itself Distributed Denial of Secrets has posted 269 gigabytes of police data online. According to a memo from the National Fusion Center Association obtained by Brian Krebs, the data were taken from state owned and operated law enforcement fusion centers, which serve to coordinate communications between state, local, federal, tribal, territorial, private law enforcement partners. The memo notes that "Preliminary analysis of the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centers, law enforcement, and other government agencies across the United States, was the source of the compromise."

Read more in:
- **krebsonsecurity.com**: 'BlueLeaks' Exposes Files from Hundreds of Police Departments
- **arstechnica.com**: Millions of documents from >200 US police agencies published in "BlueLeaks" trove
- **www.wired.com**: Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents
- **www.zdnet.com**: BlueLeaks: Data from 200 US police departments & fusion centers published online
- **www.cyberscoop.com**: 'Distributed Denial of Secrets' publishes 'Blue Leaks,' a trove of law

enforcement records
- **www.vice.com**: ‘BlueLeaks’: Group Releases 270GB of Sensitive Police Documents

Sent from my iPhone

Fwd: Data Stolen from US Law Enforcement Databases

From: Leo.Schmitz@cookcountyil.gov
To: Amar Patel <Amar.Patel@cookcountyil.gov>, Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>
Sent: June 23, 2020 7:37:01 PM CDT
Received: June 23, 2020 7:37:02 PM CDT

This affect us in any way?

Leo P. Schmitz
Chief of Public Safety
Cook County Sheriffs Department

Sent from my iPhone

E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

Begin forwarded message:

> **From:** "Leo Schmitz (Sheriff)" <Leo.Schmitz@cookcountyil.gov>
> **Date:** June 23, 2020 at 7:36:20 PM CDT
> **To:** "Arunas Buntinas (Sheriff)" <Arunas.Buntinas2@cookcountyil.gov>
> **Cc:** "Marlon Parks (Sheriff)" <Marlon.Parks@cookcountyil.gov>, "Brian White (Sheriff)" <Brian.White@cookcountyil.gov>
> **Subject: Re: Data Stolen from US Law Enforcement Databases**
>
> Did they get any of our info?
>
> Leo P. Schmitz
> Chief of Public Safety
> Cook County Sheriffs Department
>
> Sent from my iPhone
>
> E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-

mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

On Jun 23, 2020, at 5:49 PM, Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov> wrote:

Group Posts 269 GB of Data Stolen from US Law Enforcement Databases

(June 22, 2020)

A group calling itself Distributed Denial of Secrets has posted 269 gigabytes of police data online. According to a memo from the National Fusion Center Association obtained by Brian Krebs, the data were taken from state owned and operated law enforcement fusion centers, which serve to coordinate communications between state, local, federal, tribal, territorial, private law enforcement partners. The memo notes that "Preliminary analysis of the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centers, law enforcement, and other government agencies across the United States, was the source of the compromise."

Read more in:
- **krebsonsecurity.com**: 'BlueLeaks' Exposes Files from Hundreds of Police Departments
- **arstechnica.com**: Millions of documents from >200 US police agencies published in "BlueLeaks" trove
- **www.wired.com**: Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents
- **www.zdnet.com**: BlueLeaks: Data from 200 US police departments & fusion centers published online
- **www.cyberscoop.com**: 'Distributed Denial of Secrets' publishes 'Blue Leaks,' a trove of law enforcement records
- **www.vice.com**: 'BlueLeaks': Group Releases 270GB of Sensitive Police Documents

Sent from my iPhone

Fwd: Data Stolen from US Law Enforcement Databases

From: Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov>
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>
Sent: June 23, 2020 7:37:02 PM CDT
Received: June 23, 2020 7:37:03 PM CDT

This affect us in any way?

Leo P. Schmitz
Chief of Public Safety
Cook County Sheriffs Department

Sent from my iPhone

E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

Begin forwarded message:

> **From:** "Leo Schmitz (Sheriff)" <Leo.Schmitz@cookcountyil.gov>
> **Date:** June 23, 2020 at 7:36:20 PM CDT
> **To:** "Arunas Buntinas (Sheriff)" <Arunas.Buntinas2@cookcountyil.gov>
> **Cc:** "Marlon Parks (Sheriff)" <Marlon.Parks@cookcountyil.gov>, "Brian White (Sheriff)" <Brian.White@cookcountyil.gov>
> **Subject: Re: Data Stolen from US Law Enforcement Databases**
>
> Did they get any of our info?
>
> Leo P. Schmitz
> Chief of Public Safety
> Cook County Sheriffs Department
>
> Sent from my iPhone
>
> E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended

recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

On Jun 23, 2020, at 5:49 PM, Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov> wrote:

Group Posts 269 GB of Data Stolen from US Law Enforcement Databases

(June 22, 2020)

A group calling itself Distributed Denial of Secrets has posted 269 gigabytes of police data online. According to a memo from the National Fusion Center Association obtained by Brian Krebs, the data were taken from state owned and operated law enforcement fusion centers, which serve to coordinate communications between state, local, federal, tribal, territorial, private law enforcement partners. The memo notes that "Preliminary analysis of the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centers, law enforcement, and other government agencies across the United States, was the source of the compromise."

Read more in:
- **krebsonsecurity.com**: 'BlueLeaks' Exposes Files from Hundreds of Police Departments
- **arstechnica.com**: Millions of documents from >200 US police agencies published in "BlueLeaks" trove
- **www.wired.com**: Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents
- **www.zdnet.com**: BlueLeaks: Data from 200 US police departments & fusion centers published online
- **www.cyberscoop.com**: 'Distributed Denial of Secrets' publishes 'Blue Leaks,' a trove of law enforcement records
- **www.vice.com**: 'BlueLeaks': Group Releases 270GB of Sensitive Police Documents

Sent from my iPhone

Fwd: Data Stolen from US Law Enforcement Databases

From: Leo Schmitz (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D9CD12213A744B67BF85F400559CE4A7-LEO SCHMITZ>
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>
Sent: June 23, 2020 7:37:02 PM CDT
Received: June 23, 2020 7:37:03 PM CDT

This affect us in any way?

Leo P. Schmitz
Chief of Public Safety
Cook County Sheriffs Department

Sent from my iPhone

E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

Begin forwarded message:

> **From:** "Leo Schmitz (Sheriff)" <Leo.Schmitz@cookcountyil.gov>
> **Date:** June 23, 2020 at 7:36:20 PM CDT
> **To:** "Arunas Buntinas (Sheriff)" <Arunas.Buntinas2@cookcountyil.gov>
> **Cc:** "Marlon Parks (Sheriff)" <Marlon.Parks@cookcountyil.gov>, "Brian White (Sheriff)" <Brian.White@cookcountyil.gov>
> **Subject: Re: Data Stolen from US Law Enforcement Databases**
>
> Did they get any of our info?
>
> Leo P. Schmitz
> Chief of Public Safety
> Cook County Sheriffs Department
>
> Sent from my iPhone
>
> E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error,

please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

On Jun 23, 2020, at 5:49 PM, Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov> wrote:

Group Posts 269 GB of Data Stolen from US Law Enforcement Databases

(June 22, 2020)

A group calling itself Distributed Denial of Secrets has posted 269 gigabytes of police data online. According to a memo from the National Fusion Center Association obtained by Brian Krebs, the data were taken from state owned and operated law enforcement fusion centers, which serve to coordinate communications between state, local, federal, tribal, territorial, private law enforcement partners. The memo notes that "Preliminary analysis of the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centers, law enforcement, and other government agencies across the United States, was the source of the compromise."

Read more in:
- **krebsonsecurity.com**: 'BlueLeaks' Exposes Files from Hundreds of Police Departments
- **arstechnica.com**: Millions of documents from >200 US police agencies published in "BlueLeaks" trove
- **www.wired.com**: Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents
- **www.zdnet.com**: BlueLeaks: Data from 200 US police departments & fusion centers published online
- **www.cyberscoop.com**: 'Distributed Denial of Secrets' publishes 'Blue Leaks,' a trove of law enforcement records
- **www.vice.com**: 'BlueLeaks': Group Releases 270GB of Sensitive Police Documents

Sent from my iPhone

Fwd: Data Leak

From:	Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov>
To:	Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Bradley Curry (Sheriff) <Bradley.Curry@cookcountyil.gov>, Marlon Parks (Sheriff) <Marlon.Parks@cookcountyil.gov>, Brian White (Sheriff) <Brian.White@cookcountyil.gov>, Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov>
Sent:	June 23, 2020 7:52:35 PM CDT
Received:	June 23, 2020 7:52:36 PM CDT

FYI

Leo P. Schmitz
Chief of Public Safety
Cook County Sheriffs Department

Sent from my iPhone

E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

Begin forwarded message:

From: Nick Roti <nroti@chicago-hidta.org>
Date: June 23, 2020 at 7:45:28 PM CDT
To: "Leo Schmitz (Sheriff)" <Leo.Schmitz@cookcountyil.gov>
Subject: Fwd: Data Leak

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

FYI

Nicholas J. Roti
Executive Director
Chicago HIDTA
312.448.5666 Office
312.617.7237 Cell
nroti@chicago-hidta.org

Begin forwarded message:

From: "Leopold, Daniel J" <Daniel.J.Leopold@ice.dhs.gov>
Date: June 23, 2020 at 6:40:39 PM CDT
To: Brian Wolfe <mbwolfe@fbi.gov>, Leo Panepinto <Leo.Panepinto@chicagopolice.org>, "Quinn, Patrick" <patrick.quinn@chicagopolice.org>, Aaron Kustermann <aaron_kustermann@isp.state.il.us>, Darrell Aders <darrell_aders@isp.state.il.us>, "Workman, Byron" <Byron.Workman@illinois.gov>, Alison Jacobs <alison.l.jacobs2.mil@mail.mil>, James G Probst <james.g.probst.mil@mail.mil>, "dale.k.kirkendoll.mil@mail.mil" <dale.k.kirkendoll.mil@mail.mil>, Steven Artino <steven.t.artino@cbp.dhs.gov>, "robert.w.harris@dhs.gov" <robert.w.harris@dhs.gov>, Christian Hoffman <Christian.M.Hoffman@usdoj.gov>, Jim Crotty <james.m.crotty@usdoj.gov>, Patrick O'Dea <patrick.j.o'dea@usdoj.gov>, Nick Roti <nroti@chicago-hidta.org>, Jessica Ipema <Jessica.m.ipema@usdoj.gov>, "MARK.DELIA@ILLINOIS.GOV" <MARK.DELIA@ILLINOIS.GOV>, Robert Graves <rmgraves@fbi.gov>, "Worniak, Adam T. (CG) (FBI)" <atworniak@fbi.gov>, "Krumrei, Erich W. (CG) (FBI)" <ewkrumrei@fbi.gov>, Jeffrey Rauch <jdrauch@fbi.gov>, "Chellberg, Samantha (CG) (FBI)" <schellberg@fbi.gov>, "Justiniano, Robert (CG) (FBI)" <rjustiniano@fbi.gov>, "JVButhorn@uspis.gov" <JVButhorn@uspis.gov>
Cc: Daniel Leopold <daniel.j.leopold@ice.dhs.gov>
Subject: Data Leak

All, see below link related to a massive data breach exposing 24 years' worth of documents, PII, RFIs, etc. from over 200 federal, state, and local police departments. Apparently, there is 270 gigs of data.

https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

Thanks,

Dan

Daniel J. Leopold | Chief Intelligence Officer
DHS - ICE | Homeland Security Investigations | SAC Chicago
One Tower Lane, Suite 1600 | Oakbrook Terrace, Illinois 60181
(630) 441-8343 (c)(| (630) 574-4121 | daniel.j.leopold@ice.dhs.gov
Illinois| Indiana |Wisconsin

WARNING: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information.

Please inform the sender that you received this message in error and delete the message from your system.

Fwd: Data Leak

From: Leo Schmitz (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D9CD12213A744B67BF85F400559CE4A7-LEO SCHMITZ>

To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Bradley Curry (Sheriff) <Bradley.Curry@cookcountyil.gov>, Marlon Parks (Sheriff) <Marlon.Parks@cookcountyil.gov>, Brian White (Sheriff) <Brian.White@cookcountyil.gov>, Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov>

Sent: June 23, 2020 7:52:35 PM CDT

Received: June 23, 2020 7:52:36 PM CDT

FYI

Leo P. Schmitz
Chief of Public Safety
Cook County Sheriffs Department

Sent from my iPhone

E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

Begin forwarded message:

> **From:** Nick Roti <nroti@chicago-hidta.org>
> **Date:** June 23, 2020 at 7:45:28 PM CDT
> **To:** "Leo Schmitz (Sheriff)" <Leo.Schmitz@cookcountyil.gov>
> **Subject: Fwd: Data Leak**

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

FYI

Nicholas J. Roti
Executive Director
Chicago HIDTA

312.448.5666 Office
312.617.7237 Cell
nroti@chicago-hidta.org

Begin forwarded message:

From: "Leopold, Daniel J" <Daniel.J.Leopold@ice.dhs.gov>
Date: June 23, 2020 at 6:40:39 PM CDT
To: Brian Wolfe <mbwolfe@fbi.gov>, Leo Panepinto <Leo.Panepinto@chicagopolice.org>, "Quinn, Patrick" <patrick.quinn@chicagopolice.org>, Aaron Kustermann <aaron_kustermann@isp.state.il.us>, Darrell Aders <darrell_aders@isp.state.il.us>, "Workman, Byron" <Byron.Workman@illinois.gov>, Alison Jacobs <alison.l.jacobs2.mil@mail.mil>, James G Probst <james.g.probst.mil@mail.mil>, "dale.k.kirkendoll.mil@mail.mil" <dale.k.kirkendoll.mil@mail.mil>, Steven Artino <steven.t.artino@cbp.dhs.gov>, "robert.w.harris@dhs.gov" <robert.w.harris@dhs.gov>, Christian Hoffman <Christian.M.Hoffman@usdoj.gov>, Jim Crotty <james.m.crotty@usdoj.gov>, Patrick O'Dea <patrick.j.o'dea@usdoj.gov>, Nick Roti <nroti@chicago-hidta.org>, Jessica Ipema <Jessica.m.ipema@usdoj.gov>, "MARK.DELIA@ILLINOIS.GOV" <MARK.DELIA@ILLINOIS.GOV>, Robert Graves <rmgraves@fbi.gov>, "Worniak, Adam T. (CG) (FBI)" <atworniak@fbi.gov>, "Krumrei, Erich W. (CG) (FBI)" <ewkrumrei@fbi.gov>, Jeffrey Rauch <jdrauch@fbi.gov>, "Chellberg, Samantha (CG) (FBI)" <schellberg@fbi.gov>, "Justiniano, Robert (CG) (FBI)" <rjustiniano@fbi.gov>, "JVButhorn@uspis.gov" <JVButhorn@uspis.gov>
Cc: Daniel Leopold <daniel.j.leopold@ice.dhs.gov>
Subject: Data Leak

All, see below link related to a massive data breach exposing 24 years' worth of documents, PII, RFIs, etc. from over 200 federal, state, and local police departments. Apparently, there is 270 gigs of data.

https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

Thanks,

Dan

Daniel J. Leopold | Chief Intelligence Officer
DHS - ICE | Homeland Security Investigations | SAC Chicago
One Tower Lane, Suite 1600 | Oakbrook Terrace, Illinois 60181
(630) 441-8343 (c)(| (630) 574-4121 | daniel.j.leopold@ice.dhs.gov
Illinois| Indiana |Wisconsin

WARNING: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an

intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

Re: Data Stolen from US Law Enforcement Databases

From: Arunas.Buntinas2@cookcountyil.gov
To: Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov>
Sent: June 23, 2020 8:26:04 PM CDT
Received: June 23, 2020 8:26:05 PM CDT

Chief,
Checking on it now.
Arunas

On Jun 23, 2020, at 7:36 PM, Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov> wrote:

Did they get any of our info?

Leo P. Schmitz
Chief of Public Safety
Cook County Sheriffs Department

Sent from my iPhone

E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

On Jun 23, 2020, at 5:49 PM, Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov> wrote:

Group Posts 269 GB of Data Stolen from US Law Enforcement Databases

(June 22, 2020)

A group calling itself Distributed Denial of Secrets has posted 269 gigabytes of police data online. According to a memo from the National Fusion Center Association obtained by Brian Krebs, the data were taken from state owned and operated law enforcement fusion centers, which serve to coordinate communications between state, local, federal, tribal, territorial, private law enforcement partners. The memo notes that "Preliminary analysis of the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centers, law enforcement, and other government agencies across the

United States, was the source of the compromise."

Read more in:
- **krebsonsecurity.com**: 'BlueLeaks' Exposes Files from Hundreds of Police Departments
- **arstechnica.com**: Millions of documents from >200 US police agencies published in "BlueLeaks" trove
- **www.wired.com**: Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents
- **www.zdnet.com**: BlueLeaks: Data from 200 US police departments & fusion centers published online
- **www.cyberscoop.com**: 'Distributed Denial of Secrets' publishes 'Blue Leaks,' a trove of law enforcement records
- **www.vice.com**: 'BlueLeaks': Group Releases 270GB of Sensitive Police Documents

Sent from my iPhone

Re: Data Stolen from US Law Enforcement Databases

To:	Leo Schmitz (Sheriff)
Sent:	June 23, 2020 8:26:04 PM CDT
Received:	June 23, 2020 8:26:05 PM CDT

Re: Data Stolen from US Law Enforcement Databases

From: Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov>
To: Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov>
Sent: June 23, 2020 8:26:05 PM CDT
Received: June 23, 2020 8:26:07 PM CDT

Chief,
Checking on it now.
Arunas

On Jun 23, 2020, at 7:36 PM, Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov> wrote:

Did they get any of our info?

Leo P. Schmitz
Chief of Public Safety
Cook County Sheriffs Department

Sent from my iPhone

E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

On Jun 23, 2020, at 5:49 PM, Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov> wrote:

Group Posts 269 GB of Data Stolen from US Law Enforcement Databases

(June 22, 2020)

A group calling itself Distributed Denial of Secrets has posted 269 gigabytes of police data online. According to a memo from the National Fusion Center Association obtained by Brian Krebs, the data were taken from state owned and operated law enforcement fusion centers, which serve to coordinate communications between state, local, federal, tribal, territorial, private law enforcement partners. The memo notes that "Preliminary analysis of the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centers, law enforcement, and other government agencies across the

United States, was the source of the compromise."

Read more in:
- **krebsonsecurity.com**: 'BlueLeaks' Exposes Files from Hundreds of Police Departments
- **arstechnica.com**: Millions of documents from >200 US police agencies published in "BlueLeaks" trove
- **www.wired.com**: Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents
- **www.zdnet.com**: BlueLeaks: Data from 200 US police departments & fusion centers published online
- **www.cyberscoop.com**: 'Distributed Denial of Secrets' publishes 'Blue Leaks,' a trove of law enforcement records
- **www.vice.com**: 'BlueLeaks': Group Releases 270GB of Sensitive Police Documents

Sent from my iPhone

Re: Data Stolen from US Law Enforcement Databases

From: Arunas Buntinas (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=9E93BAED4821465CB7232E28F2421C49-ARUNAS BUNT>
To: Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov>
Sent: June 23, 2020 8:26:05 PM CDT
Received: June 23, 2020 8:26:06 PM CDT

Chief,
Checking on it now.
Arunas

On Jun 23, 2020, at 7:36 PM, Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov> wrote:

Did they get any of our info?

Leo P. Schmitz
Chief of Public Safety
Cook County Sheriffs Department

Sent from my iPhone

E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

On Jun 23, 2020, at 5:49 PM, Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov> wrote:

Group Posts 269 GB of Data Stolen from US Law Enforcement Databases

(June 22, 2020)

A group calling itself Distributed Denial of Secrets has posted 269 gigabytes of police data online. According to a memo from the National Fusion Center Association obtained by Brian Krebs, the data were taken from state owned and operated law enforcement fusion centers, which serve to coordinate communications between state, local, federal, tribal, territorial, private law enforcement partners. The memo notes that "Preliminary analysis of

the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centers, law enforcement, and other government agencies across the United States, was the source of the compromise."

Read more in:
- **krebsonsecurity.com**: 'BlueLeaks' Exposes Files from Hundreds of Police Departments
- **arstechnica.com**: Millions of documents from >200 US police agencies published in "BlueLeaks" trove
- **www.wired.com**: Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents
- **www.zdnet.com**: BlueLeaks: Data from 200 US police departments & fusion centers published online
- **www.cyberscoop.com**: 'Distributed Denial of Secrets' publishes 'Blue Leaks,' a trove of law enforcement records
- **www.vice.com**: 'BlueLeaks': Group Releases 270GB of Sensitive Police Documents

Sent from my iPhone

Re: Data Stolen from US Law Enforcement Databases

To:	Leo Schmitz (Sheriff), Marlon Parks (Sheriff), Brian White (Sheriff)
Sent:	June 23, 2020 8:26:05 PM CDT
Received:	June 23, 2020 8:26:06 PM CDT

Re: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

To:	Keith Morrison (Sheriff)
Cc:	Adnan Memon (Sheriff), Douglas Maclean (Sheriff)
Sent:	June 23, 2020 8:30:56 PM CDT
Received:	June 23, 2020 8:30:56 PM CDT

Re: Data Leak

To:	Leo Schmitz (Sheriff), Bradley Curry (Sheriff), Marlon Parks (Sheriff), Brian White (Sheriff), Arunas Buntinas (Sheriff), Tarry Williams (Sheriff), Amar Patel (Sheriff)
Sent:	June 23, 2020 8:51:02 PM CDT
Received:	June 23, 2020 8:51:03 PM CDT

Re: Data Leak

From:	Leo.Schmitz@cookcountyil.gov
To:	Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>
Cc:	Bradley Curry (Sheriff) <Bradley.Curry@cookcountyil.gov>, Marlon Parks (Sheriff) <Marlon.Parks@cookcountyil.gov>, Brian White (Sheriff) <Brian.White@cookcountyil.gov>, Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov>, Tarry Williams (Sheriff) <Tarry.Williams@cookcountyil.gov>
Sent:	June 23, 2020 9:48:05 PM CDT
Received:	June 23, 2020 9:48:06 PM CDT

Ten four. Thanks.

Leo P. Schmitz
Chief of Public Safety
Cook County Sheriffs Department

Sent from my iPhone

E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

On Jun 23, 2020, at 8:51 PM, Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov> wrote:

Hi,

[redacted]

[redacted]

Please let me know if any other questions. Thanks

Amar

"Security reporter Brian Krebs said that the breach took place at a Houston area web services company that "maintains several law-enforcement data centers."

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 7:10 AM
Cc: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>; Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

This is a different article from the International Association of Chiefs of Police that relates Netsentinal is a Houston service provider for Law Enforcement.

https://www.theblaze.com/news/blueleaks-hackers-release-countless-records-on-police-officers-all-searchable-by-badge-number

I think our only risk from doxing would be workforce. I pulled the attached reports last Friday and provided them to Chuck at Homeland for review.

From: Keith Morrison (Sheriff)
Sent: Tuesday, June 23, 2020 6:45 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

[redacted]

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 6:20 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 7:52 PM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Bradley Curry (Sheriff) <Bradley.Curry@cookcountyil.gov>; Marlon Parks (Sheriff) <Marlon.Parks@cookcountyil.gov>; Brian White (Sheriff) <Brian.White@cookcountyil.gov>; Arunas Buntinas (Sheriff) <Arunas.Buntinas2@cookcountyil.gov>
Subject: Fwd: Data Leak

FYI

Leo P. Schmitz
Chief of Public Safety
Cook County Sheriffs Department

Sent from my iPhone

E-MAIL CONFIDENTIALITY NOTICE: This electronic mail message, including any attachments, is for the intended recipient(s) only. This e-mail and any attachments might contain information that is confidential, legally privileged, contains law enforcement database information, or otherwise protected or exempt from disclosure under applicable law. If you are not a named recipient, or if you are named but believe that you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and promptly delete this e-mail and any attachments and copies thereof from your system. If you are not the intended recipient or are otherwise not authorized to further disclose this message and its contents, please be aware that any copying, distribution, dissemination, disclosure or other use of this e-mail and any attachments is unauthorized and prohibited. Your receipt of this message is not intended to waive any applicable privilege or claim of confidentiality, and any prohibited or unauthorized disclosure is not binding on the sender or the Cook County Sheriff's Office. Thank you for your cooperation.

Begin forwarded message:

> **From:** Nick Roti <nroti@chicago-hidta.org>
> **Date:** June 23, 2020 at 7:45:28 PM CDT
> **To:** "Leo Schmitz (Sheriff)" <Leo.Schmitz@cookcountyil.gov>
> **Subject: Fwd: Data Leak**

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

FYI

Nicholas J. Roti
Executive Director
Chicago HIDTA
312.448.5666 Office
312.617.7237 Cell
nroti@chicago-hidta.org

Begin forwarded message:

From: "Leopold, Daniel J" <Daniel.J.Leopold@ice.dhs.gov>
Date: June 23, 2020 at 6:40:39 PM CDT
To: Brian Wolfe <mbwolfe@fbi.gov>, Leo Panepinto <Leo.Panepinto@chicagopolice.org>, "Quinn, Patrick" <patrick.quinn@chicagopolice.org>, Aaron Kustermann <aaron_kustermann@isp.state.il.us>, Darrell Aders <darrell_aders@isp.state.il.us>, "Workman, Byron" <Byron.Workman@illinois.gov>, Alison Jacobs <alison.l.jacobs2.mil@mail.mil>, James G Probst <james.g.probst.mil@mail.mil>, "dale.k.kirkendoll.mil@mail.mil" <dale.k.kirkendoll.mil@mail.mil>, Steven Artino <steven.t.artino@cbp.dhs.gov>, "robert.w.harris@dhs.gov" <robert.w.harris@dhs.gov>, Christian Hoffman <Christian.M.Hoffman@usdoj.gov>, Jim Crotty <james.m.crotty@usdoj.gov>, Patrick O'Dea <patrick.j.o'dea@usdoj.gov>, Nick Roti <nroti@chicago-hidta.org>, Jessica Ipema <Jessica.m.ipema@usdoj.gov>, "MARK.DELIA@ILLINOIS.GOV" <MARK.DELIA@ILLINOIS.GOV>, Robert Graves <rmgraves@fbi.gov>, "Worniak, Adam T. (CG) (FBI)" <atworniak@fbi.gov>, "Krumrei, Erich W. (CG) (FBI)" <ewkrumrei@fbi.gov>, Jeffrey Rauch <jdrauch@fbi.gov>, "Chellberg, Samantha (CG) (FBI)" <schellberg@fbi.gov>, "Justiniano, Robert (CG) (FBI)" <rjustiniano@fbi.gov>, "JVButhorn@uspis.gov" <JVButhorn@uspis.gov>
Cc: Daniel Leopold <daniel.j.leopold@ice.dhs.gov>
Subject: Data Leak

All, see below link related to a massive data breach exposing 24 years' worth of documents, PII, RFIs, etc. from over 200 federal, state, and local police departments. Apparently, there is 270 gigs of data.

https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

Thanks,

Dan

Daniel J. Leopold | Chief Intelligence Officer
DHS - ICE | Homeland Security Investigations | SAC Chicago
One Tower Lane, Suite 1600 | Oakbrook Terrace, Illinois 60181

(630) 441-8343 (c)(| (630) 574-4121 | daniel.j.leopold@ice.dhs.gov
Illinois| Indiana |Wisconsin

WARNING: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

Re: Data Leak

To:	Amar Patel (Sheriff), Bradley Curry (Sheriff), Marlon Parks (Sheriff), Brian White (Sheriff), Arunas Buntinas (Sheriff)
Cc:	Bradley Curry (Sheriff), Marlon Parks (Sheriff), Brian White (Sheriff), Arunas Buntinas (Sheriff), Tarry Williams (Sheriff)
Sent:	June 23, 2020 9:48:06 PM CDT
Received:	June 23, 2020 9:48:06 PM CDT

Tasks

From:	Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>
To:	Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent:	June 23, 2020 10:09:34 PM CDT
Received:	June 23, 2020 10:09:35 PM CDT
Attachments:	WORK_062320.xlsx

Attached.

Jonathan Springborn
Cook County Sheriff's Office
Sheriff's Information Technology Unit
3026 S. California, Chicago, IL 60608
Jonathan.Springborn@cookcounyil.gov
(773) 674-6850 – Sheriff Help Desk
(312) 339-2995 – Mobile
www.cookcountysheriff.org

Tasks

From:	Jonathan Springborn (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=32F2A0A9AA124C638CA1784E3422B464-JONATHAN SP>
To:	Keith Morrison (Keith.Morrison@cookcountyil.gov) <Keith.Morrison@cookcountyil.gov>
Sent:	June 23, 2020 10:09:34 PM CDT
Received:	June 23, 2020 10:09:00 PM CDT
Attachments:	WORK_062320.xlsx

Attached.

Jonathan Springborn
Cook County Sheriff's Office
Sheriff's Information Technology Unit
3026 S. California, Chicago, IL 60608
Jonathan.Springborn@cookcounyil.gov
(773) 674-6850 – Sheriff Help Desk
(312) 339-2995 – Mobile
www.cookcountysheriff.org

Good Morning! The Power of Information - Law Enforcement News of the Day: June 24, 2020

From:	Ness and Associates Law Enforcement Daily News <jness23@cox.net>
To:	Phyllis <phyllis.tillis@cookcountyil.gov>, Phyllis Tillis (Sheriff) <Phyllis.Tillis@cookcountyil.gov>
Sent:	June 24, 2020 5:59:51 AM CDT
Received:	June 24, 2020 5:59:59 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

View this email in your browser

Your daily source for what's interesting and news worthy around the country and the rest of the world

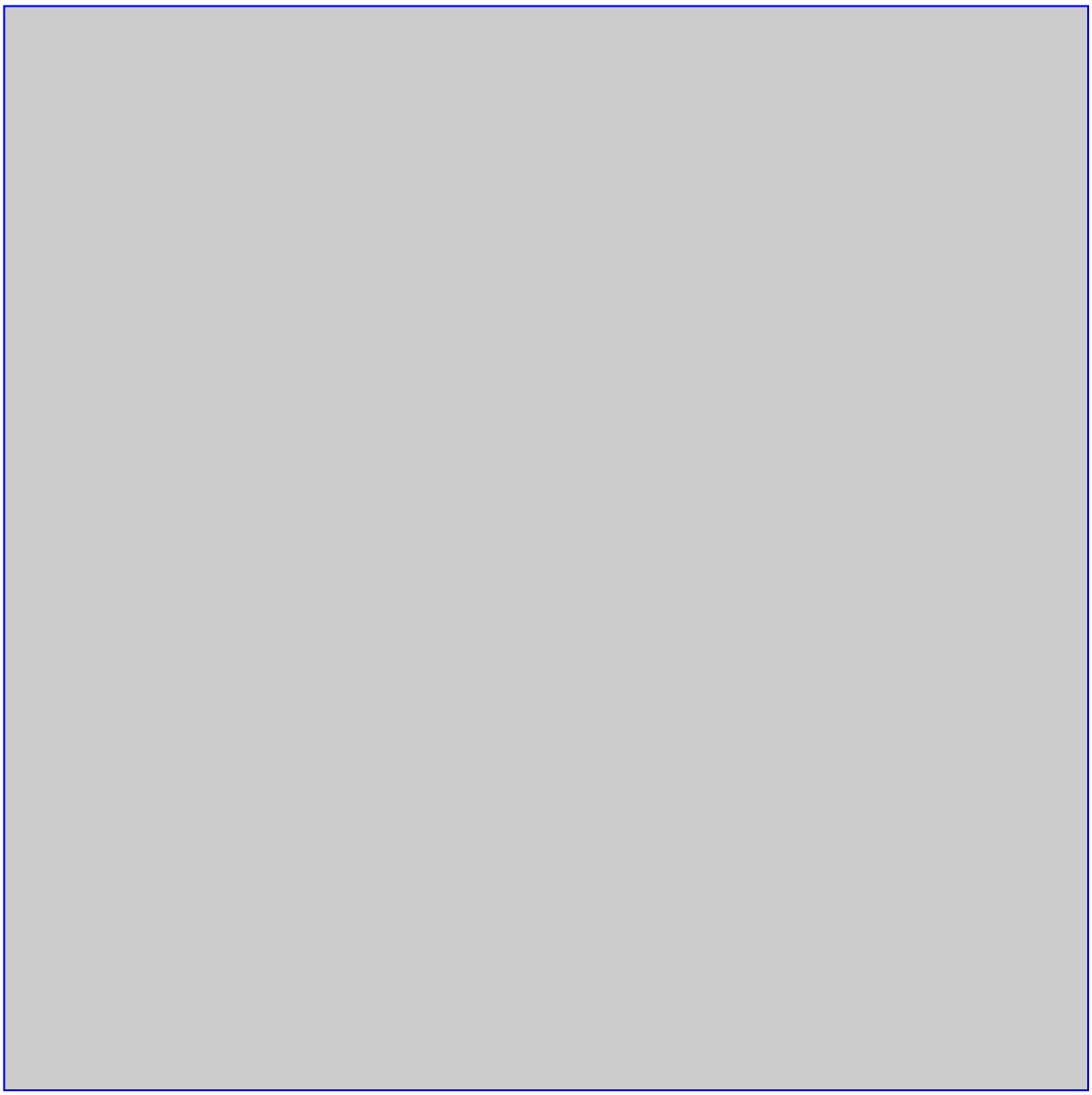
Daily News & Updates for Wednesday June 24, 2020

THOUGHT FOR THE DAY

“When we long for life without difficulties, remind us that oaks grow strong in contrary winds and diamonds are made under pressure.” Peter Marshall

Minneapolis Police Chief Medaria Arradondo on George Floyd's killing, policies during protests and reform for his department

On Memorial Day, a white Minneapolis police officer knelt on a black man's neck until he was unresponsive. The killing of George Floyd sparked the protests we've seen around the country.With Minneapolis on edge and under scrutiny, the pressure is on the city's police chief, Medaria Arradondo, a 30-year veteran and the first black man to head the mostly white police department. He fired the four officers involved within 24 hours. We spoke with the chief remotely, discussing the events of May 25, the video that ignited it all and the police response, which started with a lie.



Want to reform the police? Hire more women

It was a moment that captured national attention and revealed an important lesson about police reform.

A Fort Lauderdale, Florida, policeman, facing off against a line of yelling demonstrators, sticks his finger in the face of a protester. He then turns toward a kneeling woman, her hands raised in protest. The officer suddenly lunges and shoves her.

Then, a female officer appears. She swats her male colleague back toward a line of patrol cars, waving her arm and appearing to upbraid him for what he did.

"Thank you!" a protester shouts at Officer Krystle Smith, who won praise for her actions on social media and from police leaders around the country.

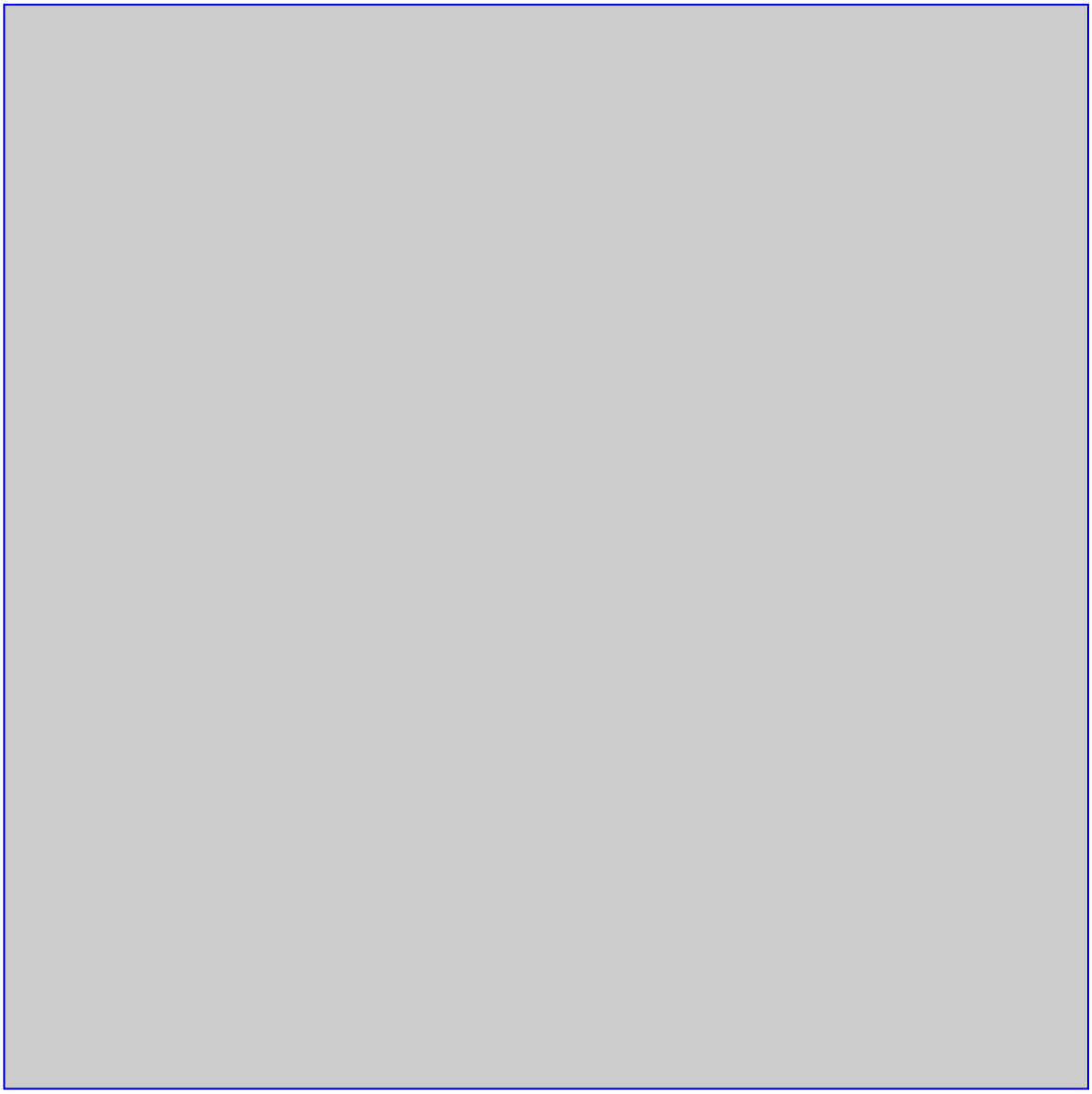
Neither Smith nor Officer Steven Pohorence, who is suspended pending an outside investigation, were allowed to comment on the incident.

"I was proud of her," said Ivonne Roman, the former police chief in Newark, New Jersey, who has been fighting for years to push her profession to hire more women. "That is why we need more women in policing. Statistically, they do not escalate; they de-escalate."

As protests over the police killing of George Floyd have refocused national attention on police abuses and use of force, law enforcement experts and leaders say one powerful reform would be simple: Hire more women.

Women make up only about one out of every eight sworn police officers nationwide, according to federal statistics.

\



LAPD officers call in absent for nearly 700

transit-policing shifts in one week

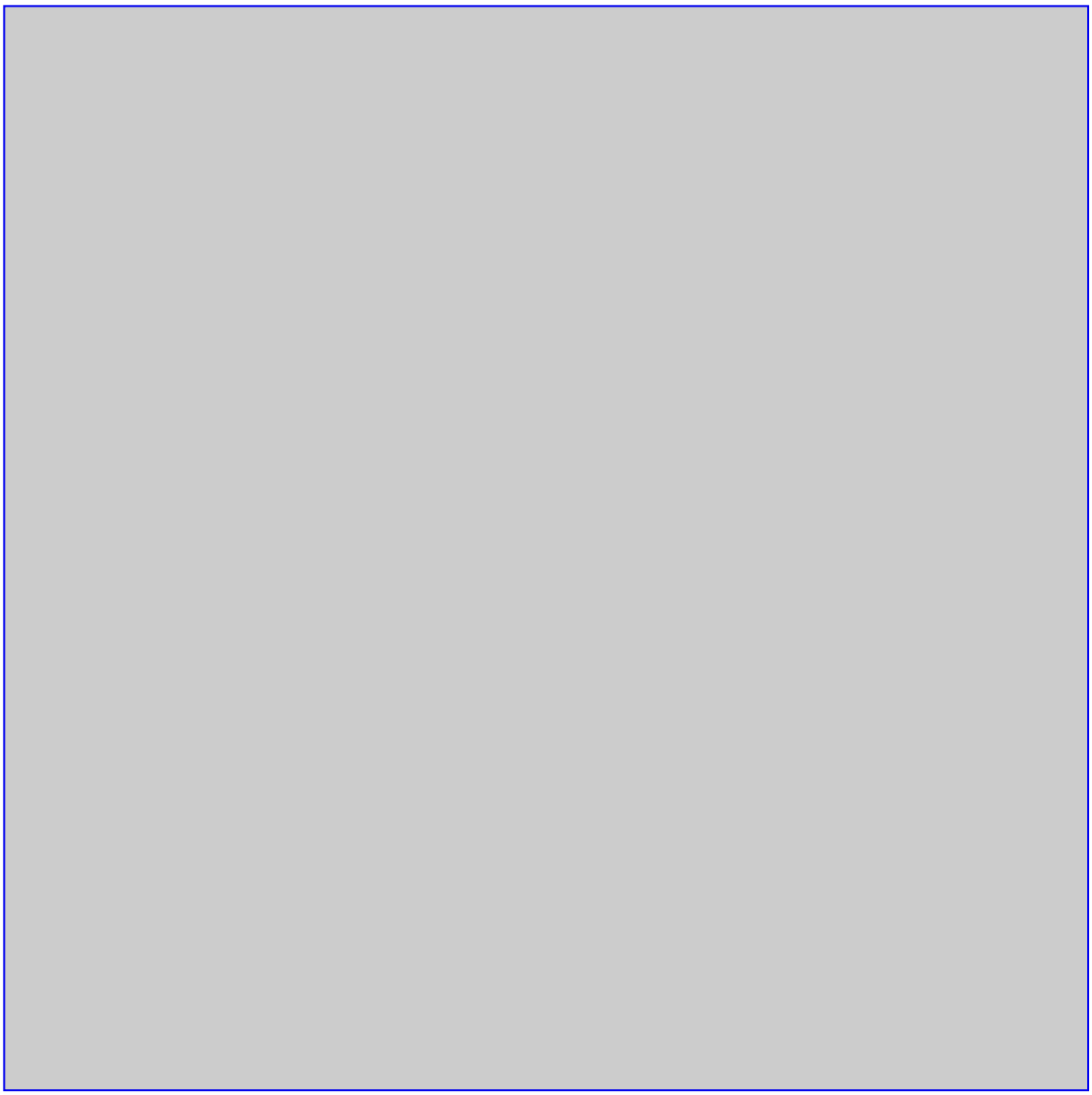
Dozens of policing shifts on Los Angeles County's transit system went unfilled last week after Los Angeles Police Department officers called in absent nearly 700 times, the Metropolitan Transportation Authority said.

The absences, for overtime shifts with premium pay, came after Chief Michel Moore temporarily froze overtime for the LAPD.

The department spent $40 million in overtime during a week of protests over police brutality, systemic racism and the death of George Floyd, Moore told officers earlier this month. He said future overtime would be paid out with time off, rather than cash.

The LAPD's $369-million, five-year contract to patrol Metro buses and trains in L.A. includes an agreement to staff 1,008 shifts per week, said LAPD spokesman Josh Rubenstein. Those shifts are filled by officers working overtime, he said.

From June 12 to June 19, LAPD officers called in absent for 696 transit policing shifts, Metro spokesman Rick Jager said. Most were filled through substitutes, but 171 went unfilled, he said.



Saying Chicago police uphold ‘racist and white supremacist values,’ DePaul tutors refuse to work with officers taking classes, call for university to cut ties with department

After weeks of student calls to end educational programs that serve members of the Chicago Police Department, DePaul University Provost Salma Ghanem turned aside the demands on Monday, saying in a statement that “the actions of a few do not represent the (CPD officers) we teach.”

The provost’s statement also included an account from an unnamed police officer who said she was “devastated” by the students’ appeal.

“As a CPD Latina I am proud to be who I am and for the past 12 years have worked tirelessly throughout my career to make a difference and I can bet my life

savings that many officers (enrolled at DePaul) share the same feelings," she wrote.

Ghanem's statement didn't sit well with some who want DePaul to sever ties with CPD and Chicago's Fraternal Order of Police Lodge 7. Junior Aneesah Shealey, who was one of the first to criticize educational programs the school offers to the police union, said students will continue to organize to reverse the decision.

"We're trying to emphasize that you can't separate the person from the career," she said. "It doesn't matter that there are good cops. They're still protecting the ones committing the acts of violence."

A DePaul spokeswoman said Ghanem was not available for an interview, and declined to provide other officials to answer questions on the school's behalf.

Black men plan Southfield Michigan march to

protest police brutality

SOUTHFIELD, Mich. (AP) — A march designed to unite Black men while protesting police brutality and racial injustice is scheduled for next week in suburban Detroit.

Organizers say the planned peaceful protest on June 28 will begin at Hope United Methodist Church in Southfield, just north of Detroit, and end at the city's municipal offices.

A voter registration drive will be held, and participants also will be encouraged to complete the 2020 census.

Peaceful protests, demonstrations and unrest have spread to cities around the U.S. following the May 25 death of George Floyd in Minneapolis. A white police officer pressed his knee into Floyd's neck for several minutes, even after the handcuffed Black man stopped moving and pleading for air.

Chicago’s violent weekend renews search for answers in a tense city, points again to entrenched problems

New Chicago police Superintendent David Brown has been in his post for just two months, but his walk to a lectern at police headquarters had a familiar feel Monday.

Another weekend of stunning bloodshed in Chicago had given way to another round of police and city leaders grasping for explanations.

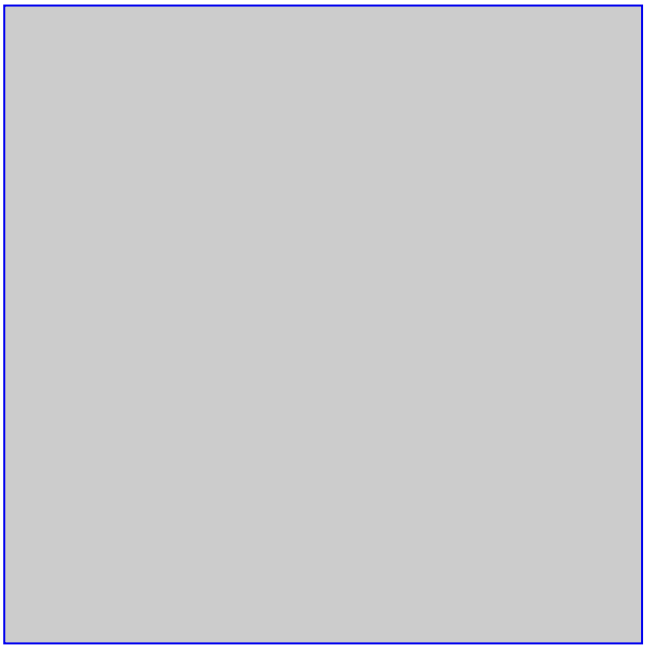
“On the heels of Father’s Day, I come to you again with obviously a high level of frustration and disappointment,” Brown said at a press briefing.

This time, on the first official summer weekend of the year, it was 106 people shot, 14 of them fatally — including a 3-year-old boy.

The tally between Friday afternoon and early Monday marked the most people shot in one weekend here since at least 2012, and the violence took a particular toll on children. Twelve of those shot were younger than 18 years old. Five of them died, including two walking into their backyard after going to get candy at a corner shop.

Six shootings involved three or more victims. One drive-by shooting early Monday in the East Garfield Park neighborhood injured five, including a 16-year-old girl who was left in critical condition.

And while shootings were seen across the city, those who work at the front lines of reducing violence also were left to consider what's happening on blocks that have borne the brunt of the problem for decades. Chicago is an agitated place, they said, dealing with the stress of a global pandemic, recent civil unrest and the fallout from decades of neglect and abandonment in some neighborhoods.



Massive attack on police: 'Blueleaks' hackers release 'hundreds of thousands' of private records on officers

Hackers have leaked highly sensitive police files from over 200 police departments across the country, according to a Business Insider report Monday.

All files are reportedly searchable by badge number. Activist group DDoSecrets published what the outlet calls "hundreds of gigabytes' worth of potentially sensitive files" from police departments across the United States. The group has called the information dump "BlueLeaks."

The group compiled the records, disseminating them into a searchable database that can pull up private information from a police badge number. Many of the files include information such as memos, emails, and officers' personal information.

The group shared information on Twitter regarding the data dump.

It wrote, "RELEASE: #BlueLeaks (269 GB) Ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources. Among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more."

‘The officers feel like they can’t win’: Tampa chief responds to police criticism

At a brief press conference Monday, Tampa police Chief Brian Dugan painted a picture of a beleaguered police force, worn down by weeks of protests and media scrutiny.

“The police, we always have everybody’s back and nobody has our back,” he said. “Right now the officers feel like they can’t win. And I would have to agree with them.”

He said demonstrations against police brutality that have blocked traffic and sometimes led to tense stand-offs have created a dilemma for police. Officers have kept their distance from recent protests in an effort to diffuse tension, but Dugan said that wasn't sustainable.

"Police are in a very tough spot — if we show up to people who are just merely exercising their First Amendment rights, it turns into a clash and police are the bad guys," he said. "But we also now have people who are complaining about the lack of a police presence at these protests."

He highlighted two recent incidents unrelated to the protests where officers were injured: On Saturday night, officers responded to calls of shots fired at 15th Street N and 26th Avenue N, only to encounter a crowd of hundreds who threw bottles at officers and jumped on a police vehicle. One officer was struck on the left side of his face and went to the hospital with a laceration. No shooting victim was found and Dugan described it as an "ambush" at a block party.

41 Cities, Many Sources: How False Antifa Rumors Spread Locally

In recent weeks, as demonstrations against racism spread across the country, residents in at least 41 U.S. cities and towns became alarmed by rumors that the loose collective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, they contacted their local law enforcement for help.

In each case, it was for a threat that never appeared.

President Trump has spread some unfounded rumors about antifa to a national audience — including his accusation, without evidence, that a 75-year-old Buffalo protester who was hospitalized after being knocked down by a police officer could be "an antifa provocateur."

But on the local level, the source of the false information has usually been more

subtle, and shows the complexity of stunting misinformation online. The bad information often first appears in a Twitter or Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking app Nextdoor and community texting networks. These posts can fall under the radar of the tech companies and online fact checkers.

Garcetti under fire for handling of police brutality protests

The police union has called him unstable. Activists accuse him of supporting racist

institutions. Even longtime allies said his decisions during the recent protests over police brutality hurt Los Angeles' communities of color.

Mayor Eric Garcetti's handling of the demonstrations and his subsequent actions drew criticism from an array of groups, wide pushback unseen during his seven years leading the city.

Garcetti, known for avoiding political risk, has appeared at times whipsawed by the protests and their aftermath.

"When you're being fired on politically from all sides, not sure exactly how to move because you know you can't make everybody happy?" said Isaac Bryan, director of the Black Policy Project at UCLA. "I can imagine that's a frustrating place for him."

As police and demonstrators clashed in the Fairfax district last month, Garcetti said he didn't plan to request the National Guard. Hours later, he did. Angering the police union, he unveiled plans to cut the Police Department, after defending its size days earlier.

The Latest: Police: 2 dead, 7 wounded in N Carolina shooting

CHARLOTTE, N.C. — Authorities in North Carolina say a shooting at an impromptu block party has left two people dead and seven others wounded.

Charlotte-Mecklenburg Police Deputy Chief Johnny Jennings told reporters early Monday the shooting happened around midnight at a block party that was a continuation of Juneteenth celebrations. Jennings said police responding to a pedestrian call found hundreds of people in the streets.

After authorities arrived, several shots were fired and the crowd scattered.

Jennings said five people were hit by cars while running away from the shooting.

He said there was evidence of multiple shooters.

Further details weren't immediately available.

Ex-FBI agent charged with hoarding top-secret government documents

A former FBI special agent who worked for years in Chicago’s organized crime division has been charged with stealing sensitive government documents and hoarding them in his home after retirement.

Yen Cham Yung, who achieved top government security clearance during his lengthy career, was arrested in Colorado earlier this week and is scheduled to be brought to Chicago to face the charges.

Yung, 57, was accused in a criminal complaint unsealed Tuesday of illegally keeping hundreds of documents without consent, including sensitive information about undercover informants, surveillance of gang activity and email threads between FBI supervisors concerning organized crime investigations.

The complaint also alleged Yung violated national security protocols by keeping a copy of a memorandum of understanding between the CIA and FBI “regarding the

activities of those agencies overseas and domestically.”
The memorandum had been accessed in 2009 at the Chicago FBI headquarters by someone using Yung’s credentials, according to the complaint.
The charges do not allege Yung sold or disseminated any of the information.

Officers find mannequin dressed in police uniform hanging from Jacksonville overpass

JACKSONVILLE, Fla. – Jacksonville police on Saturday morning found a mannequin dressed in a law enforcement uniform hanging from an overpass, authorities said.
About 6:20 a.m., according to the Jacksonville Sheriff’s Office, police were called

to a potential suicide by hanging on the Interstate 95 overpass near Zoo Parkway. Police said they then discovered it was actually a mannequin dressed in an New York Police Department uniform with a pig mask.

“About 6 a.m., we was coming on 95, and first, I thought it was a body and my heart completely dropped,” said Jacksonville resident Lamont Ross, who is a medical transportation driver, along with his wife. “Immediately we turned around.”

Kamri Merriweather also saw the mannequin on her way home from working a 12-hour shift.

“My entire heart dropped. It just sank. I was not sure what to do. I was nerve wrecked, scared and at the same time confused. I could not believe, out of my entire life, I would ever see anything like that,” Merriweather said.

Detectives said the mannequin will be processed for DNA.

30 cases of deadly police force will get state review to ensure independent investigation

A statewide investigation will be done into 30 cases where police killed people this year to ensure law enforcement agencies are complying with a new law requiring independent investigations, Washington State Attorney General Bob Ferguson announced Tuesday.

The inquiry was prompted by Pierce County Sheriff's Department's lapses to follow Initiative 940 while looking into the March 3 death of Manuel Ellis as he was detained by Tacoma police.

"Pierce County's admitted failure to comply with the requirements of I-940 is deeply troubling," Ferugson said in a statement. "I hope our inquiry will find that law enforcement agencies across the state, unlike Pierce County, are following the law that requires independent, transparent investigations into the use of deadly force."

There are no known instances of other investigations not complying with the law, Ferguson said.

Once the review is complete, the Attorney General's Office will release its findings to the public.

No timeline was given.

GOP senator introduces measure to curb legal shield for law enforcement

GOP Senator Mike Braun of Indiana is rolling out legislation aimed at reforming the powerful legal shield that protects police officers and other government officials from being sued for misconduct, an issue that has become a focal point in the debate over policing raging across the country.

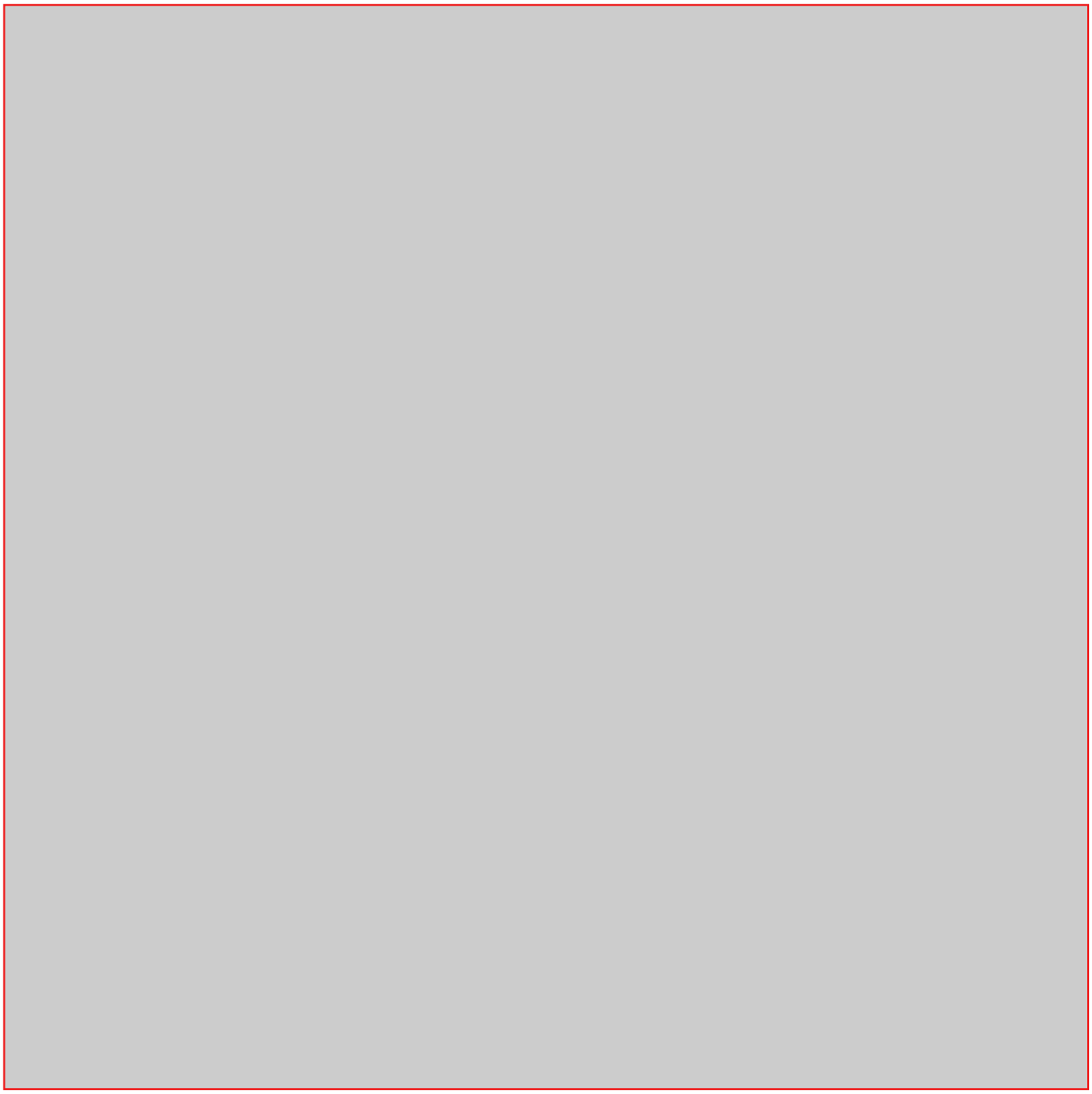
The measure to be introduced by Braun on Tuesday targets the legal doctrine known as qualified immunity, which protects government officials from civil lawsuits unless victims can show officers violated "clearly established" constitutional or statutory rights. Created by the Supreme Court, the doctrine has faced heightened criticism in recent years due to the high bar victims must reach to hold law enforcement accountable for use of excessive force.

Braun's proposal scales qualified immunity back and says that government

officials, including police, can claim qualified immunity only when they can prove their alleged conduct had previously been authorized by federal or state law, or when a court has found the alleged unlawful conduct was consistent with the U.S. Constitution and federal laws.

The bill would also ensure that municipalities are held accountable for their employees' misconduct.

"It's time Congress does their job to establish a qualified immunity law that defends law enforcement, while protecting the rights of the people," Braun said in a statement. The Indiana senator called the criteria law enforcement must satisfy to assert qualified immunity under his bill "a meaningful change that will help law enforcement and the citizens they protect."



The Law Enforcement News of the Day is a compilation of daily news articles selected from thousands of sources by the editors of Ness & Associates. Ness & Associates are not liable for the use of or reliance on any information contained in these articles. The presence of advertising does not endorse, nor imply endorsement of, any products or services by Ness & Associates.

Copyright © 2020 Ness & Associates

Have an interesting article you would like to share? email jness23@cox.net

Copyright © 2020 Ness Associates, All rights reserved.
You are receiving this email because you opted in via our website.

Our mailing address is:
Ness Associates
9241 E Grandview St
Mesa, AZ 85207-4318

Add us to your address book

Want to change how you receive these emails?
You can update your preferences or unsubscribe from this list.

Good Morning! The Power of Information - Law Enforcement News of the Day: June 24, 2020

To:	Phyllis Tillis (Sheriff)
Sent:	June 24, 2020 5:59:51 AM CDT
Received:	June 24, 2020 5:59:59 AM CDT

IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: jennifer.warren@cookcountyil.gov, Jennifer Warren (Sheriff) <jennifer.warren@cookcountyil.gov>

Sent: June 24, 2020 6:25:01 AM CDT
Received: June 24, 2020 6:25:06 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Jennifer Warren

Wednesday, June 24, 2020

POLICING & POLICY

Top Senate Democrats Dismiss Republican Policing Reform Bill

The AP (6/23, Mascaro) reports Congress is "hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away." Ahead of a test vote Wednesday, Senate Majority Leader McConnell "acknowledged it may fall short," and the GOP bill's author, Sen. Tim Scott (R-SC), "warned against a partisan, political debate that chisels away confidence in the nation's institutions." Reuters (6/23, Morgan) similarly says "Democrats and Republicans...found themselves in a partisan deadlock on Tuesday."

AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform. The AP (6/23, Long, Fingerhut) reports that Americans "overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation's criminal justice system." The new AP-NORC poll "also finds there is strong support for penalizing officers who engage in racially biased policing."

Confronting Nazi Legacy Part Of German Police Training

The New York Times (6/23, Bennhold, Eddy) reports that "visiting a former concentration camp is mandatory for every

future police officer in Berlin." To the Times, it is "one of the ways in which policing was fundamentally overhauled in Germany after World War II."

Rhode Island Governor Signs Ban On 3D-Printed Weapons, "Ghost Guns"

The AP (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo "on Tuesday signed into law bills that ban 3D-printed guns and so-called 'ghost guns' in the state." The bills "are 'a matter of public health,' she said." The bills "were approved by the legislature last week," and "make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up $10,000. The laws take effect in 30 days."

Seattle, Washington To End Anti-Loitering Law

Fox News (6/23, Carter) reports, "Seattle is moving to end a longstanding city law that allowed police to arrest someone for loitering, if they are also suspected of being a possible drug offender or sex worker." According to Fox News, "The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color."

Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The AP (6/23, Nadler, Amy) reports, "Georgia's legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp's desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders." According to the AP, "The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support."

The impact of an officer's line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

Review documents and resources.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Law Enforcement Concerned About Rash Of Gun-Store Robberies

Politico (6/23, Swan) reports, "A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country." According to Politico, "In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau's assistant director of field operations Tom Chittum told POLITICO. 'It's a lot of guns,' Chittum said in an interview. 'It's the biggest spike I have ever seen of gun store burglaries.'" Chittum "said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists."

Gun Violence Spikes In New York City

The New York Times (6/23, Southall, Macfarquhar) reports, "It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year." The city "logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions." New York "is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers." On Monday, Mayor Bill de Blasio "announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department."

Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The Columbia (SC) State (6/23, Monk) reports, "More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing." According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests "were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018." FBI South Carolina SAC Jody Norris said, "Even in the midst of a pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina." Also reporting are WACH-TV Columbia, SC (6/23, Lanahan) and WIS-TV Columbia, SC (6/23, Greene).

GLOBAL SECURITY

Suicide Bomber Targets Turkish Military Base In Somalia

The New York Times (6/23, Mohamed, Dahir) reports, "Two people were killed after a suicide bomber detonated his explosives outside Turkey's largest overseas military base in Mogadishu on Tuesday." The attack, which the Times says "bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway."

The AP (6/23, Guled) says Tuesday's attack marks "the first time Turkey's largest overseas military base has been attacked by the al-Qaida-linked al-Shabab extremist group," which "quickly claimed responsibility, according to its Radio al-Furqan affiliate."

Secret Recordings Detail Neo-Nazi Group's Grooming, Recruiting Process

Fox News (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show "senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them." The founder of the group, American Rinaldo Nazzaro, "who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons." Fox reports Nazzaro "purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago."

ALSO IN THE NEWS

FCC To Vote Next Month On Making "988" New Suicide Hotline Number

The AP (6/23, Arbel) reports the FCC "will vote in July on whether to make '988' the number to reach a suicide prevention hotline." The Commission explained that "phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected."

TUESDAY'S LEAD STORIES

- **US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police**
- **Swedish Rape Conviction Rates Rise 75% After Change In Law**
- **"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers**

- **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to jennifer.warren@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: brian.white@cookcountyil.gov, Brian White (Sheriff) <Brian.White@cookcountyil.gov>

Sent: June 24, 2020 6:25:01 AM CDT
Received: June 24, 2020 6:25:07 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Brian White Wednesday, June 24, 2020

POLICING & POLICY

Top Senate Democrats Dismiss Republican Policing Reform Bill

The AP (6/23, Mascaro) reports Congress is "hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away." Ahead of a test vote Wednesday, Senate Majority Leader McConnell "acknowledged it may fall short," and the GOP bill's author, Sen. Tim Scott (R-SC), "warned against a partisan, political debate that chisels away confidence in the nation's institutions." Reuters (6/23, Morgan) similarly says "Democrats and Republicans...found themselves in a partisan deadlock on Tuesday."

AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform. The AP (6/23, Long, Fingerhut) reports that Americans "overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation's criminal justice system." The new AP-NORC poll "also finds there is strong support for penalizing officers who engage in racially biased policing."

Confronting Nazi Legacy Part Of German Police Training

The New York Times (6/23, Bennhold, Eddy) reports that "visiting a former concentration camp is mandatory for every

future police officer in Berlin." To the Times, it is "one of the ways in which policing was fundamentally overhauled in Germany after World War II."

Rhode Island Governor Signs Ban On 3D-Printed Weapons, "Ghost Guns"

The AP (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo "on Tuesday signed into law bills that ban 3D-printed guns and so-called 'ghost guns' in the state." The bills "are 'a matter of public health,' she said." The bills "were approved by the legislature last week," and "make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up $10,000. The laws take effect in 30 days."

Seattle, Washington To End Anti-Loitering Law

Fox News (6/23, Carter) reports, "Seattle is moving to end a longstanding city law that allowed police to arrest someone for loitering, if they are also suspected of being a possible drug offender or sex worker." According to Fox News, "The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color."

Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The AP (6/23, Nadler, Amy) reports, "Georgia's legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp's desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders." According to the AP, "The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support."

The impact of an officer's line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

Review documents and resources.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Law Enforcement Concerned About Rash Of Gun-Store Robberies

Politico (6/23, Swan) reports, "A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country." According to Politico, "In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau's assistant director of field operations Tom Chittum told POLITICO. 'It's a lot of guns,' Chittum said in an interview. 'It's the biggest spike I have ever seen of gun store burglaries.'" Chittum "said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists."

Gun Violence Spikes In New York City

The New York Times (6/23, Southall, Macfarquhar) reports, "It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year." The city "logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions." New York "is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers." On Monday, Mayor Bill de Blasio "announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department."

Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The Columbia (SC) State (6/23, Monk) reports, "More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing." According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests "were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018." FBI South Carolina SAC Jody Norris said, "Even in the midst of a pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina." Also reporting are WACH-TV Columbia, SC (6/23, Lanahan) and WIS-TV Columbia, SC (6/23, Greene).

GLOBAL SECURITY

Suicide Bomber Targets Turkish Military Base In Somalia

The New York Times (6/23, Mohamed, Dahir) reports, "Two people were killed after a suicide bomber detonated his explosives outside Turkey's largest overseas military base in Mogadishu on Tuesday." The attack, which the Times says "bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway."

The AP (6/23, Guled) says Tuesday's attack marks "the first time Turkey's largest overseas military base has been attacked by the al-Qaida-linked al-Shabab extremist group," which "quickly claimed responsibility, according to its Radio al-Furqan affiliate."

Secret Recordings Detail Neo-Nazi Group's Grooming, Recruiting Process

Fox News (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show "senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them." The founder of the group, American Rinaldo Nazzaro, "who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons." Fox reports Nazzaro "purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago."

ALSO IN THE NEWS

FCC To Vote Next Month On Making "988" New Suicide Hotline Number

The AP (6/23, Arbel) reports the FCC "will vote in July on whether to make '988' the number to reach a suicide prevention hotline." The Commission explained that "phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected."

TUESDAY'S LEAD STORIES

- **US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police**
- **Swedish Rape Conviction Rates Rise 75% After Change In Law**
- **"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers**

- **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to brian.white@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: keith.morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: June 24, 2020 6:25:01 AM CDT
Received: June 24, 2020 6:25:07 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Keith Morrison Wednesday, June 24, 2020

POLICING & POLICY

Top Senate Democrats Dismiss Republican Policing Reform Bill

The AP (6/23, Mascaro) reports Congress is "hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away." Ahead of a test vote Wednesday, Senate Majority Leader McConnell "acknowledged it may fall short," and the GOP bill's author, Sen. Tim Scott (R-SC), "warned against a partisan, political debate that chisels away confidence in the nation's institutions." Reuters (6/23, Morgan) similarly says "Democrats and Republicans...found themselves in a partisan deadlock on Tuesday."

AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform. The AP (6/23, Long, Fingerhut) reports that Americans "overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation's criminal justice system." The new AP-NORC poll "also finds there is strong support for penalizing officers who engage in racially biased policing."

Confronting Nazi Legacy Part Of German Police Training

The New York Times (6/23, Bennhold, Eddy) reports that "visiting a former concentration camp is mandatory for every

future police officer in Berlin." To the Times, it is "one of the ways in which policing was fundamentally overhauled in Germany after World War II."

Rhode Island Governor Signs Ban On 3D-Printed Weapons, "Ghost Guns"

The AP (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo "on Tuesday signed into law bills that ban 3D-printed guns and so-called 'ghost guns' in the state." The bills "are 'a matter of public health,' she said." The bills "were approved by the legislature last week," and "make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up $10,000. The laws take effect in 30 days."

Seattle, Washington To End Anti-Loitering Law

Fox News (6/23, Carter) reports, "Seattle is moving to end a longstanding city law that allowed police to arrest someone for loitering, if they are also suspected of being a possible drug offender or sex worker." According to Fox News, "The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color."

Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The AP (6/23, Nadler, Amy) reports, "Georgia's legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp's desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders." According to the AP, "The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support."

The impact of an officer's line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

Review documents and resources.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Law Enforcement Concerned About Rash Of Gun-Store Robberies

Politico (6/23, Swan) reports, "A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country." According to Politico, "In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau's assistant director of field operations Tom Chittum told POLITICO. 'It's a lot of guns,' Chittum said in an interview. 'It's the biggest spike I have ever seen of gun store burglaries.'" Chittum "said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists."

Gun Violence Spikes In New York City

The New York Times (6/23, Southall, Macfarquhar) reports, "It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year." The city "logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions." New York "is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers." On Monday, Mayor Bill de Blasio "announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department."

Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The Columbia (SC) State (6/23, Monk) reports, "More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing." According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests "were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018." FBI South Carolina SAC Jody Norris said, "Even in the midst of a pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina." Also reporting are WACH-TV Columbia, SC (6/23, Lanahan) and WIS-TV Columbia, SC (6/23, Greene).

GLOBAL SECURITY

Suicide Bomber Targets Turkish Military Base In Somalia

The New York Times (6/23, Mohamed, Dahir) reports, "Two people were killed after a suicide bomber detonated his explosives outside Turkey's largest overseas military base in Mogadishu on Tuesday." The attack, which the Times says "bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway."

The AP (6/23, Guled) says Tuesday's attack marks "the first time Turkey's largest overseas military base has been attacked by the al-Qaida-linked al-Shabab extremist group," which "quickly claimed responsibility, according to its Radio al-Furqan affiliate."

Secret Recordings Detail Neo-Nazi Group's Grooming, Recruiting Process

Fox News (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show "senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them." The founder of the group, American Rinaldo Nazzaro, "who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons." Fox reports Nazzaro "purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago."

ALSO IN THE NEWS

FCC To Vote Next Month On Making "988" New Suicide Hotline Number

The AP (6/23, Arbel) reports the FCC "will vote in July on whether to make '988' the number to reach a suicide prevention hotline." The Commission explained that "phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected."

TUESDAY'S LEAD STORIES

- **US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police**
- **Swedish Rape Conviction Rates Rise 75% After Change In Law**
- **"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers**

- **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to keith.morrison@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: noureen.kapadia@cookcountyil.gov, Noureen Kapadia (Sheriff) <Noureen.Kapadia@cookcountyil.gov>

Sent: June 24, 2020 6:25:01 AM CDT
Received: June 24, 2020 6:25:07 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Noureen Kapadia

Wednesday, June 24, 2020

POLICING & POLICY

Top Senate Democrats Dismiss Republican Policing Reform Bill

The AP (6/23, Mascaro) reports Congress is "hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away." Ahead of a test vote Wednesday, Senate Majority Leader McConnell "acknowledged it may fall short," and the GOP bill's author, Sen. Tim Scott (R-SC), "warned against a partisan, political debate that chisels away confidence in the nation's institutions." Reuters (6/23, Morgan) similarly says "Democrats and Republicans...found themselves in a partisan deadlock on Tuesday."

AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform. The AP (6/23, Long, Fingerhut) reports that Americans "overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation's criminal justice system." The new AP-NORC poll "also finds there is strong support for penalizing officers who engage in racially biased policing."

Confronting Nazi Legacy Part Of German Police Training

The New York Times (6/23, Bennhold, Eddy) reports that "visiting a former concentration camp is mandatory for every

future police officer in Berlin." To the Times, it is "one of the ways in which policing was fundamentally overhauled in Germany after World War II."

Rhode Island Governor Signs Ban On 3D-Printed Weapons, "Ghost Guns"

The AP (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo "on Tuesday signed into law bills that ban 3D-printed guns and so-called 'ghost guns' in the state." The bills "are 'a matter of public health,' she said." The bills "were approved by the legislature last week," and "make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up $10,000. The laws take effect in 30 days."

Seattle, Washington To End Anti-Loitering Law

Fox News (6/23, Carter) reports, "Seattle is moving to end a longstanding city law that allowed police to arrest someone for loitering, if they are also suspected of being a possible drug offender or sex worker." According to Fox News, "The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color."

Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The AP (6/23, Nadler, Amy) reports, "Georgia's legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp's desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders." According to the AP, "The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support."

The impact of an officer's line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

Review documents and resources.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Law Enforcement Concerned About Rash Of Gun-Store Robberies

Politico (6/23, Swan) reports, "A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country." According to Politico, "In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau's assistant director of field operations Tom Chittum told POLITICO. 'It's a lot of guns,' Chittum said in an interview. 'It's the biggest spike I have ever seen of gun store burglaries.'" Chittum "said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists."

Gun Violence Spikes In New York City

The New York Times (6/23, Southall, Macfarquhar) reports, "It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year." The city "logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions." New York "is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers." On Monday, Mayor Bill de Blasio "announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department."

Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The Columbia (SC) State (6/23, Monk) reports, "More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing." According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests "were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018." FBI South Carolina SAC Jody Norris said, "Even in the midst of a pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina." Also reporting are WACH-TV Columbia, SC (6/23, Lanahan) and WIS-TV Columbia, SC (6/23, Greene).

GLOBAL SECURITY

Suicide Bomber Targets Turkish Military Base In Somalia

The New York Times (6/23, Mohamed, Dahir) reports, "Two people were killed after a suicide bomber detonated his explosives outside Turkey's largest overseas military base in Mogadishu on Tuesday." The attack, which the Times says "bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway."

The AP (6/23, Guled) says Tuesday's attack marks "the first time Turkey's largest overseas military base has been attacked by the al-Qaida-linked al-Shabab extremist group," which "quickly claimed responsibility, according to its Radio al-Furqan affiliate."

Secret Recordings Detail Neo-Nazi Group's Grooming, Recruiting Process

Fox News (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show "senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them." The founder of the group, American Rinaldo Nazzaro, "who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons." Fox reports Nazzaro "purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago."

ALSO IN THE NEWS

FCC To Vote Next Month On Making "988" New Suicide Hotline Number

The AP (6/23, Arbel) reports the FCC "will vote in July on whether to make '988' the number to reach a suicide prevention hotline." The Commission explained that "phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected."

TUESDAY'S LEAD STORIES

- **US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police**
- **Swedish Rape Conviction Rates Rise 75% After Change In Law**
- **"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers**

- **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to noureen.kapadia@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: thomas.conley@cookcountyil.gov, Thomas Conley (Sheriff) <Thomas.Conley@cookcountyil.gov>

Sent: June 24, 2020 6:25:01 AM CDT
Received: June 24, 2020 6:25:08 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Thomas Conley Wednesday, June 24, 2020

POLICING & POLICY

Top Senate Democrats Dismiss Republican Policing Reform Bill

The AP (6/23, Mascaro) reports Congress is "hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away." Ahead of a test vote Wednesday, Senate Majority Leader McConnell "acknowledged it may fall short," and the GOP bill's author, Sen. Tim Scott (R-SC), "warned against a partisan, political debate that chisels away confidence in the nation's institutions." Reuters (6/23, Morgan) similarly says "Democrats and Republicans...found themselves in a partisan deadlock on Tuesday."

AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform. The AP (6/23, Long, Fingerhut) reports that Americans "overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation's criminal justice system." The new AP-NORC poll "also finds there is strong support for penalizing officers who engage in racially biased policing."

Confronting Nazi Legacy Part Of German Police Training

The New York Times (6/23, Bennhold, Eddy) reports that "visiting a former concentration camp is mandatory for every

future police officer in Berlin." To the Times, it is "one of the ways in which policing was fundamentally overhauled in Germany after World War II."

Rhode Island Governor Signs Ban On 3D-Printed Weapons, "Ghost Guns"

The AP (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo "on Tuesday signed into law bills that ban 3D-printed guns and so-called 'ghost guns' in the state." The bills "are 'a matter of public health,' she said." The bills "were approved by the legislature last week," and "make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up $10,000. The laws take effect in 30 days."

Seattle, Washington To End Anti-Loitering Law

Fox News (6/23, Carter) reports, "Seattle is moving to end a longstanding city law that allowed police to arrest someone for loitering, if they are also suspected of being a possible drug offender or sex worker." According to Fox News, "The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color."

Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The AP (6/23, Nadler, Amy) reports, "Georgia's legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp's desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders." According to the AP, "The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support."

The impact of an officer's line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

Review documents and resources.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Law Enforcement Concerned About Rash Of Gun-Store Robberies

Politico (6/23, Swan) reports, "A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country." According to Politico, "In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau's assistant director of field operations Tom Chittum told POLITICO. 'It's a lot of guns,' Chittum said in an interview. 'It's the biggest spike I have ever seen of gun store burglaries.'" Chittum "said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists."

Gun Violence Spikes In New York City

The New York Times (6/23, Southall, Macfarquhar) reports, "It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year." The city "logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions." New York "is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers." On Monday, Mayor Bill de Blasio "announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department."

Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The Columbia (SC) State (6/23, Monk) reports, "More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing." According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests "were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018." FBI South Carolina SAC Jody Norris said, "Even in the midst of a pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina." Also reporting are WACH-TV Columbia, SC (6/23, Lanahan) and WIS-TV Columbia, SC (6/23, Greene).

GLOBAL SECURITY

Suicide Bomber Targets Turkish Military Base In Somalia

The New York Times (6/23, Mohamed, Dahir) reports, "Two people were killed after a suicide bomber detonated his explosives outside Turkey's largest overseas military base in Mogadishu on Tuesday." The attack, which the Times says "bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway."

The AP (6/23, Guled) says Tuesday's attack marks "the first time Turkey's largest overseas military base has been attacked by the al-Qaida-linked al-Shabab extremist group," which "quickly claimed responsibility, according to its Radio al-Furqan affiliate."

Secret Recordings Detail Neo-Nazi Group's Grooming, Recruiting Process

Fox News (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show "senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them." The founder of the group, American Rinaldo Nazzaro, "who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons." Fox reports Nazzaro "purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago."

ALSO IN THE NEWS

FCC To Vote Next Month On Making "988" New Suicide Hotline Number

The AP (6/23, Arbel) reports the FCC "will vote in July on whether to make '988' the number to reach a suicide prevention hotline." The Commission explained that "phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected."

TUESDAY'S LEAD STORIES

- **US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police**
- **Swedish Rape Conviction Rates Rise 75% After Change In Law**
- **"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers**

- **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to thomas.conley@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: theresa.olson@cookcountyil.gov, Theresa Olson (Sheriff) <Theresa.Olson@cookcountyil.gov>

Sent: June 24, 2020 6:25:01 AM CDT
Received: June 24, 2020 6:25:08 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Theresa Olson Wednesday, June 24, 2020

POLICING & POLICY

Top Senate Democrats Dismiss Republican Policing Reform Bill

The AP (6/23, Mascaro) reports Congress is "hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away." Ahead of a test vote Wednesday, Senate Majority Leader McConnell "acknowledged it may fall short," and the GOP bill's author, Sen. Tim Scott (R-SC), "warned against a partisan, political debate that chisels away confidence in the nation's institutions." Reuters (6/23, Morgan) similarly says "Democrats and Republicans...found themselves in a partisan deadlock on Tuesday."

AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform. The AP (6/23, Long, Fingerhut) reports that Americans "overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation's criminal justice system." The new AP-NORC poll "also finds there is strong support for penalizing officers who engage in racially biased policing."

Confronting Nazi Legacy Part Of German Police Training

The New York Times (6/23, Bennhold, Eddy) reports that "visiting a former concentration camp is mandatory for every

future police officer in Berlin." To the Times, it is "one of the ways in which policing was fundamentally overhauled in Germany after World War II."

Rhode Island Governor Signs Ban On 3D-Printed Weapons, "Ghost Guns"

The AP (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo "on Tuesday signed into law bills that ban 3D-printed guns and so-called 'ghost guns' in the state." The bills "are 'a matter of public health,' she said." The bills "were approved by the legislature last week," and "make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up $10,000. The laws take effect in 30 days."

Seattle, Washington To End Anti-Loitering Law

Fox News (6/23, Carter) reports, "Seattle is moving to end a longstanding city law that allowed police to arrest someone for loitering, if they are also suspected of being a possible drug offender or sex worker." According to Fox News, "The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color."

Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The AP (6/23, Nadler, Amy) reports, "Georgia's legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp's desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders." According to the AP, "The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support."

The impact of an officer's line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

Review documents and resources.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Law Enforcement Concerned About Rash Of Gun-Store Robberies

Politico (6/23, Swan) reports, "A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country." According to Politico, "In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau's assistant director of field operations Tom Chittum told POLITICO. 'It's a lot of guns,' Chittum said in an interview. 'It's the biggest spike I have ever seen of gun store burglaries.'" Chittum "said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists."

Gun Violence Spikes In New York City

The New York Times (6/23, Southall, Macfarquhar) reports, "It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year." The city "logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions." New York "is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers." On Monday, Mayor Bill de Blasio "announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department."

Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The Columbia (SC) State (6/23, Monk) reports, "More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing." According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests "were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018." FBI South Carolina SAC Jody Norris said, "Even in the midst of a pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina." Also reporting are WACH-TV Columbia, SC (6/23, Lanahan) and WIS-TV Columbia, SC (6/23, Greene).

GLOBAL SECURITY

Suicide Bomber Targets Turkish Military Base In Somalia

The New York Times (6/23, Mohamed, Dahir) reports, "Two people were killed after a suicide bomber detonated his explosives outside Turkey's largest overseas military base in Mogadishu on Tuesday." The attack, which the Times says "bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway."

The AP (6/23, Guled) says Tuesday's attack marks "the first time Turkey's largest overseas military base has been attacked by the al-Qaida-linked al-Shabab extremist group," which "quickly claimed responsibility, according to its Radio al-Furqan affiliate."

Secret Recordings Detail Neo-Nazi Group's Grooming, Recruiting Process

Fox News (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show "senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them." The founder of the group, American Rinaldo Nazzaro, "who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons." Fox reports Nazzaro "purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago."

ALSO IN THE NEWS

FCC To Vote Next Month On Making "988" New Suicide Hotline Number

The AP (6/23, Arbel) reports the FCC "will vote in July on whether to make '988' the number to reach a suicide prevention hotline." The Commission explained that "phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected."

TUESDAY'S LEAD STORIES

- **US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police**
- **Swedish Rape Conviction Rates Rise 75% After Change In Law**
- **"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers**

- **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to theresa.olson@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

Fwd: IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.

From: Sean.Gleason@cookcountyil.gov
To: 2020CriminalInvestigationsSupervisors@cookcounty.onmicrosoft.com, 2020 Criminal Investigations Supervisors <2020CriminalInvestigationsSupervisors@cookcounty.onmicrosoft.com>
Sent: June 24, 2020 8:25:29 AM CDT
Received: June 24, 2020 8:25:31 AM CDT

Sent from my iPhone

Begin forwarded message:

From: The IACP <TheLead@iacp.bulletinmedia.com>
Date: June 24, 2020 at 6:25:08 AM CDT
To: "Sean Gleason (Sheriff)" <Sean.Gleason@cookcountyil.gov>
Subject: IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Sean Gleason Wednesday, June 24, 2020

POLICING & POLICY

Top Senate Democrats Dismiss Republican Policing Reform Bill

The AP (6/23, Mascaro) reports Congress is "hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away." Ahead of a test vote Wednesday, Senate Majority Leader McConnell "acknowledged it may fall short," and the GOP bill's author, Sen. Tim Scott (R-SC), "warned against a partisan, political debate that chisels away confidence in the nation's institutions." Reuters (6/23, Morgan) similarly says "Democrats and Republicans...found themselves in a partisan deadlock on Tuesday."

AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform. The AP (6/23, Long, Fingerhut) reports that Americans "overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation's criminal justice system." The new AP-NORC poll "also finds there is strong support for penalizing officers who engage in racially biased policing."

Confronting Nazi Legacy Part Of German Police Training

The New York Times (6/23, Bennhold, Eddy) reports that "visiting a former concentration camp is mandatory for every future police officer in Berlin." To the Times, it is "one of the ways in which policing was fundamentally overhauled in Germany after World War II."

Rhode Island Governor Signs Ban On 3D-Printed Weapons, "Ghost Guns"

The AP (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo "on Tuesday signed into law bills that ban 3D-printed guns and so-called 'ghost guns' in the state." The bills "are 'a matter of public health,' she said." The bills "were approved by the legislature last week," and "make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up $10,000. The laws take effect in 30 days."

Seattle, Washington To End Anti-Loitering Law

Fox News (6/23, Carter) reports, "Seattle is moving to end a longstanding city law that allowed police to arrest someone for loitering, if they are also suspected of being a possible drug offender or sex worker." According to Fox News, "The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color."

Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The AP (6/23, Nadler, Amy) reports, "Georgia's legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp's desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders." According to the AP, "The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support."

The impact of an officer's line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

Review documents and resources.

Connect with the IACP online: **IACP Event Calendar:**

CRIME & DRUGS

Law Enforcement Concerned About Rash Of Gun-Store Robberies

Politico (6/23, Swan) reports, "A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country." According to Politico, "In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau's assistant director of field operations Tom Chittum told POLITICO. 'It's a lot of guns,' Chittum said in an interview. 'It's the biggest spike I have ever seen of gun store burglaries.'" Chittum "said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists."

Gun Violence Spikes In New York City

The New York Times (6/23, Southall, Macfarquhar) reports, "It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year." The city "logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions." New York "is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers." On Monday, Mayor Bill de Blasio "announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department."

Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The Columbia (SC) State (6/23, Monk) reports, "More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing." According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests "were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018." FBI South Carolina SAC Jody Norris said, "Even in the midst of a pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina." Also reporting are WACH-TV Columbia, SC (6/23, Lanahan) and WIS-TV Columbia, SC (6/23, Greene).

GLOBAL SECURITY

Suicide Bomber Targets Turkish Military Base In Somalia

The New York Times (6/23, Mohamed, Dahir) reports, "Two people were killed after a suicide bomber detonated his explosives outside Turkey's largest overseas military base in Mogadishu on Tuesday." The attack, which the Times says "bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway."

The AP (6/23, Guled) says Tuesday's attack marks "the first time Turkey's largest overseas military base has been

attacked by the al-Qaida-linked al-Shabab extremist group," which "quickly claimed responsibility, according to its Radio al-Furqan affiliate."

Secret Recordings Detail Neo-Nazi Group's Grooming, Recruiting Process

Fox News (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show "senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them." The founder of the group, American Rinaldo Nazzaro, "who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons." Fox reports Nazzaro "purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago."

ALSO IN THE NEWS

FCC To Vote Next Month On Making "988" New Suicide Hotline Number

The AP (6/23, Arbel) reports the FCC "will vote in July on whether to make '988' the number to reach a suicide prevention hotline." The Commission explained that "phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected."

TUESDAY'S LEAD STORIES

- **US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police**
- **Swedish Rape Conviction Rates Rise 75% After Change In Law**
- **"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers**
- **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to sean.gleason@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

Fwd: IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.

From: Sean Gleason (Sheriff) <Sean.Gleason@cookcountyil.gov>
To: 2020 Criminal Investigations Supervisors <2020CriminalInvestigationsSupervisors@cookcounty.onmicrosoft.com>
Sent: June 24, 2020 8:25:31 AM CDT
Received: June 24, 2020 8:25:32 AM CDT

Sent from my iPhone

Begin forwarded message:

From: The IACP <TheLead@iacp.bulletinmedia.com>
Date: June 24, 2020 at 6:25:08 AM CDT
To: "Sean Gleason (Sheriff)" <Sean.Gleason@cookcountyil.gov>
Subject: IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Sean Gleason Wednesday, June 24, 2020

POLICING & POLICY

Top Senate Democrats Dismiss Republican Policing Reform Bill

The AP (6/23, Mascaro) reports Congress is "hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away." Ahead of a test vote Wednesday, Senate Majority Leader McConnell "acknowledged it may fall short," and the GOP bill's author, Sen. Tim Scott (R-SC), "warned against a partisan, political debate that chisels away confidence in the nation's institutions." Reuters (6/23, Morgan) similarly says "Democrats and Republicans...found themselves in a partisan deadlock on Tuesday."

AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform. The AP (6/23, Long, Fingerhut) reports that Americans "overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation's criminal justice system." The new AP-NORC poll "also finds there is strong support for penalizing officers who engage in racially biased policing."

Confronting Nazi Legacy Part Of German Police Training

The New York Times (6/23, Bennhold, Eddy) reports that "visiting a former concentration camp is mandatory for every future police officer in Berlin." To the Times, it is "one of the ways in which policing was fundamentally overhauled in Germany after World War II."

Rhode Island Governor Signs Ban On 3D-Printed Weapons, "Ghost Guns"

The AP (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo "on Tuesday signed into law bills that ban 3D-printed guns and so-called 'ghost guns' in the state." The bills "are 'a matter of public health,' she said." The bills "were approved by the legislature last week," and "make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up $10,000. The laws take effect in 30 days."

Seattle, Washington To End Anti-Loitering Law

Fox News (6/23, Carter) reports, "Seattle is moving to end a longstanding city law that allowed police to arrest someone for loitering, if they are also suspected of being a possible drug offender or sex worker." According to Fox News, "The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color."

Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The AP (6/23, Nadler, Amy) reports, "Georgia's legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp's desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders." According to the AP, "The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support."

The impact of an officer's line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

Review documents and resources.

Connect with the IACP online: **IACP Event Calendar:**

CRIME & DRUGS

Law Enforcement Concerned About Rash Of Gun-Store Robberies

Politico (6/23, Swan) reports, "A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country." According to Politico, "In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau's assistant director of field operations Tom Chittum told POLITICO. 'It's a lot of guns,' Chittum said in an interview. 'It's the biggest spike I have ever seen of gun store burglaries.'" Chittum "said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists."

Gun Violence Spikes In New York City

The New York Times (6/23, Southall, Macfarquhar) reports, "It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year." The city "logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions." New York "is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers." On Monday, Mayor Bill de Blasio "announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department."

Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The Columbia (SC) State (6/23, Monk) reports, "More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing." According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests "were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018." FBI South Carolina SAC Jody Norris said, "Even in the midst of a pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina." Also reporting are WACH-TV Columbia, SC (6/23, Lanahan) and WIS-TV Columbia, SC (6/23, Greene).

GLOBAL SECURITY

Suicide Bomber Targets Turkish Military Base In Somalia

The New York Times (6/23, Mohamed, Dahir) reports, "Two people were killed after a suicide bomber detonated his explosives outside Turkey's largest overseas military base in Mogadishu on Tuesday." The attack, which the Times says "bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway."

The AP (6/23, Guled) says Tuesday's attack marks "the first time Turkey's largest overseas military base has been

attacked by the al-Qaida-linked al-Shabab extremist group," which "quickly claimed responsibility, according to its Radio al-Furqan affiliate."

Secret Recordings Detail Neo-Nazi Group's Grooming, Recruiting Process

Fox News (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show "senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them." The founder of the group, American Rinaldo Nazzaro, "who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons." Fox reports Nazzaro "purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago."

ALSO IN THE NEWS

FCC To Vote Next Month On Making "988" New Suicide Hotline Number

The AP (6/23, Arbel) reports the FCC "will vote in July on whether to make '988' the number to reach a suicide prevention hotline." The Commission explained that "phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected."

TUESDAY'S LEAD STORIES

- **US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police**
- **Swedish Rape Conviction Rates Rise 75% After Change In Law**
- **"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers**
- **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to sean.gleason@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

Fwd: IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.

To: 2020 Criminal Investigations Supervisors
Sent: June 24, 2020 8:25:31 AM CDT
Received: June 24, 2020 8:25:32 AM CDT

Fwd: IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.

From:	Sean Gleason (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=396114C9D4C0432BA9B9583095EE4990-SEAN GLEASO>
To:	2020 Criminal Investigations Supervisors <2020CriminalInvestigationsSupervisors@cookcounty.onmicrosoft.com>
Sent:	June 24, 2020 8:25:31 AM CDT
Received:	June 24, 2020 8:25:32 AM CDT

Sent from my iPhone

Begin forwarded message:

From: The IACP <TheLead@iacp.bulletinmedia.com>
Date: June 24, 2020 at 6:25:08 AM CDT
To: "Sean Gleason (Sheriff)" <Sean.Gleason@cookcountyil.gov>
Subject: IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Sean Gleason Wednesday, June 24, 2020

POLICING & POLICY

Top Senate Democrats Dismiss Republican Policing Reform Bill

The AP (6/23, Mascaro) reports Congress is "hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away." Ahead of a test vote Wednesday, Senate Majority Leader McConnell "acknowledged it may fall short," and the GOP bill's author, Sen. Tim Scott (R-SC), "warned against a partisan, political debate that chisels away confidence in the nation's institutions." Reuters (6/23, Morgan) similarly says "Democrats and Republicans...found themselves in a partisan deadlock on Tuesday."

AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform. The AP (6/23, Long, Fingerhut) reports that Americans "overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation's criminal justice system." The new AP-NORC poll "also finds there is strong support for penalizing officers who engage in racially biased policing."

Confronting Nazi Legacy Part Of German Police Training

The New York Times (6/23, Bennhold, Eddy) reports that "visiting a former concentration camp is mandatory for every future police officer in Berlin." To the Times, it is "one of the ways in which policing was fundamentally overhauled in Germany after World War II."

Rhode Island Governor Signs Ban On 3D-Printed Weapons, "Ghost Guns"

The AP (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo "on Tuesday signed into law bills that ban 3D-printed guns and so-called 'ghost guns' in the state." The bills "are 'a matter of public health,' she said." The bills "were approved by the legislature last week," and "make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up $10,000. The laws take effect in 30 days."

Seattle, Washington To End Anti-Loitering Law

Fox News (6/23, Carter) reports, "Seattle is moving to end a longstanding city law that allowed police to arrest someone for loitering, if they are also suspected of being a possible drug offender or sex worker." According to Fox News, "The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color."

Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The AP (6/23, Nadler, Amy) reports, "Georgia's legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp's desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders." According to the AP, "The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support."

The impact of an officer's line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

Review documents and resources.

Connect with the IACP online: **IACP Event Calendar:**

CRIME & DRUGS

Law Enforcement Concerned About Rash Of Gun-Store Robberies

Politico (6/23, Swan) reports, "A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country." According to Politico, "In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau's assistant director of field operations Tom Chittum told POLITICO. 'It's a lot of guns,' Chittum said in an interview. 'It's the biggest spike I have ever seen of gun store burglaries.'" Chittum "said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists."

Gun Violence Spikes In New York City

The New York Times (6/23, Southall, Macfarquhar) reports, "It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year." The city "logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions." New York "is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers." On Monday, Mayor Bill de Blasio "announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department."

Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The Columbia (SC) State (6/23, Monk) reports, "More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing." According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests "were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018." FBI South Carolina SAC Jody Norris said, "Even in the midst of a pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina." Also reporting are WACH-TV Columbia, SC (6/23, Lanahan) and WIS-TV Columbia, SC (6/23, Greene).

GLOBAL SECURITY

Suicide Bomber Targets Turkish Military Base In Somalia

The New York Times (6/23, Mohamed, Dahir) reports, "Two people were killed after a suicide bomber detonated his explosives outside Turkey's largest overseas military base in Mogadishu on Tuesday." The attack, which the Times says "bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway."

The AP (6/23, Guled) says Tuesday's attack marks "the first time Turkey's largest overseas military base has been

attacked by the al-Qaida-linked al-Shabab extremist group," which "quickly claimed responsibility, according to its Radio al-Furqan affiliate."

Secret Recordings Detail Neo-Nazi Group's Grooming, Recruiting Process

Fox News (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show "senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them." The founder of the group, American Rinaldo Nazzaro, "who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons." Fox reports Nazzaro "purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago."

ALSO IN THE NEWS

FCC To Vote Next Month On Making "988" New Suicide Hotline Number

The AP (6/23, Arbel) reports the FCC "will vote in July on whether to make '988' the number to reach a suicide prevention hotline." The Commission explained that "phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected."

TUESDAY'S LEAD STORIES

- **US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police**
- **Swedish Rape Conviction Rates Rise 75% After Change In Law**
- **"Blueleaks" Hackers Release "Hundreds Of Thousands" Of Private Records On Officers**
- **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to sean.gleason@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

<!

The CyberWire 6.24.20: Twitter bans DDoSecrets. A look at Hidden Cobra. Sino-Australian cyber tension. Election security. Criminals need t.v. too.

From: The CyberWire <editor@thecyberwire.com>

To: Keith.Morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: June 24, 2020 10:29:36 AM CDT

Received: June 24, 2020 10:29:50 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

More signal, less noise.

SPONSORED BY RECORDED FUTURE:

Get real-time security intelligence at no cost.

We recently launched Recorded Future Express — a free browser extension for security teams. Use Express over any web-based SIEM, vulnerability management solution, security blog, and more to put real-time security intelligence at your fingertips. Instantly prioritize alerts, incidents, and vulnerabilities based on real-time risk scores from the world's largest commercial collection platform. Sign up now.

Daily briefing.

June 24, 2020.

SUMMARY

By the CyberWire staff

Twitter told ZDNet that the social network has permanently suspended the @DDoSecrets

Twitter account, an account belonging to the group responsible for BlueLeaks, because DDoSecrets violated Twitter's policy against distribution of hacked material.

ReversingLabs offers a walk through the tools North Korea's Hidden Cobra (also known as the Lazarus Group) uses. The lesson the researchers draw is that it's possible to develop a rich picture of a threat actor from a starting point of publicly available intelligence.

Channel News writes that Beijing is expected to retaliate for Canberra's strong hint that Chinese intelligence services are hacking targets in Australia on a large scale. The response is expected to take the form of tariffs and bans on certain Australian exports.

The Washington Post calls Kentucky's primary elections yesterday a success story worthy of emulation.

A lot of people, during the lockdowns and stay-at-home plans that many jurisdictions have imposed or recommended during the pandemic, have turned to indoor amusement to pass the time. Like watching far too much television, and that's true not only in the larger world, but in the underworld as well. Digital Shadows has noticed an interesting development in the anglophone cybercriminal platform Nulled: its gangland proprietors have begun offering a livestreaming service, "Nulledflix," to its members. The service offers television, "blockbuster" movies, and various "memes." It comes with a chat feature through which members can exchange tips, comments, and so forth. The point seems to be building underworld brand loyalty. And even criminals like to binge-watch T.V.

[250]

SPONSORED BY GDIT:

Secure your mission with the GDIT Cyber Stack, our ecosystem of cyber capabilities.

Notes.

Today's issue includes events affecting Australia, Austria, Brazil, China, Germany, India, Ireland, the Democratic People's Republic of Korea, New Zealand, Switzerland, the United Kingdom, and the United States.

Word Notes Wednesday: DevSecOps

DevSecOps (noun). Development Security Operations. The collapsing of traditional IT operations, code deployment operations, and security operations, into a single and cohesive system of systems that delivers infrastructure as code.

SPONSORED BY MCAFEE:

Transition your enterprise to a secured, remote work environment

with McAfee

Most companies aren't prepared to secure data and assets for a surge of remote employees. Whether your VPN is over capacity, new cloud services are coming on-board, or new devices need protection, we have you covered during this critical time. McAfee is offering 3-month subscriptions for Endpoint Protection, Unified Cloud Edge, and CASB to help you scale security to your remote employees. Learn more about these offers at mcafee.com/workfromhome.

ON THE PODCAST

In today's CyberWire Daily Podcast, out later this afternoon, we speak with our partners at the Johns Hopkins University's Information Security Institute, as Joe Carrigan discusses the Ripple20 vulnerabilities. Our guest, as we continue Canon Week, is Joseph Menn, author of *Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World*.

And Caveat is also up. In this episode, "Code is law," Dave's got the story of how the FBI used open source intelligence to track down an alleged arsonist, Ben describes a facial recognition test that took place at the Rose Bowl, and later in the show our conversation with Maureen Webb on her forthcoming book, *Coding Democracy: How Hackers Are Disrupting Power, Surveillance, and Authoritarianism*.

SPONSORED EVENTS

Cyber Security Summit Virtual Power Hours (Online, June 23 - 25, 2020) Senior Level Executives are invited to the Cyber Summit Virtual Power Hours. Learn from Industry Experts from The FBI, DHS, U.S. Secret Service & leading cyber solution providers as they discuss the latest security challenges & develop cyber security battle plans in today's unprecedented times. You will receive 1 CPE / CEU credit by attending. Free to register with code: CyberWire20 at CyberSummitUSA.com.

Improving Cyber-Oriented Education (Online, June 25, 2020) The Cyberspace Solarium Commission (CSC) recently released a report that proposes a strategy of layered cyber deterrence. Tune in to hear from CSC Commissioners and Industry leaders to discuss the report's findings, educational aspects, and opportunities to improve Cyber-oriented education.

FutureCon Virtual Eastern Conference (Online, June 30, 2020) This virtual event features thought-provoking presentations by Industry Security Leaders, esteemed Keynote Speakers, and a Panel Session discussion with experienced professionals and a talented team who are at the forefront of cutting edge strategies for Cybersecurity defense. 100% off promo code: CYBERWIRE

IoT Integrator Summit: Securing Edge Computing (Online, July 14 - 16, 2020) A virtual summit to help IoT Integrators learn more about advances and updates in IoT security and discover new methods for architecting IoT solutions for your organization or your clients.

RSA Conference APJ July 15-17, 2020 - A Virtual Learning Experience (Online, July 15 - 17, 2020) The world's leading cybersecurity event is going virtual 15-17 July. Join your peers and industry experts for three days of insights. Watch over 50 sessions live during Singapore business hours—or stream them later. Register today for free.

SELECTED READING

Cyber Attacks, Threats, and Vulnerabilities

Hidden Cobra - from a shed skin to the viper's nest (ReversingLabs) Enriching public threat intelligence

Twitter bans DDoSecrets account over 'BlueLeaks' police data dump (ZDNet) Twitter said DDoSecrets account leaked and promoted BlueLeaks, a huge collection of files stolen from...

SixLittleMonkeys Malware Resurfaces with with API-like Programming Enhancements (MSSP Alert) SixLittleMonkeys, an advanced persistent threat (APT) actor, applies API -style coding to its malware,...

Find MORE on our website.

Security Patches, Mitigations, and Software Updates

Windows 10's Mail app is deleting Gmail users' emails (BetaNews) An update from last month seems to have introduced a bug into the Mail app which is causing problems...

Cyber Trends

The Cost of Privacy Report 2020 (Okta) Reporting on the State of Digital Identity in 2020.

The Indelible Impact of COVID-19 on Cybersecurity (Bitdefender) Half of infosec professionals (50%) revealed that their organisations didn't have a contingency plan...

Internet Security Report - Q1 2020 (WatchGuard Technologies) The Threat Lab team analyzes data from WatchGuard's Firebox Feed, internal and partner threat intelligence,...

Find MORE on our website.

Marketplace

WSJ News Exclusive | Dell Explores Spinoff of $50 Billion Stake in VMware (Wall Street Journal) Dell is considering a spinoff and other options for its stake in the cloud-software giant, as the PC...

SecurityGate.io announces Series A funding with Houston Ventures for accelerating innovation to transform cybersecurity management in OT/ICS operational environments (PR Newswire) SecurityGate.io, a cybersecurity software company that helps organizations become leaders and experts...

Atos to acquire Paladion (ETCIO.com) This acquisition will bring Managed Detection and Response capabilities to the Atos portfolio.

Find MORE on our website.

Products, Services, and Solutions

YouAttest Launches First Cloud-Based Identity Auditing and Compliance Solution for Okta's Identity Cloud (PR Newswire) YouAttest, an innovator in the Identity Governance & Administration (IGA) market today announced the...

Armis Launches New Global Reseller Channel Program (PR Newswire) Armis®, the leading enterprise IoT security company, today announced the Armis Reseller Channel (ARC)...

ZL Technologies Solves Compliance Challenges for Financial Institutions with Advancements to its Platform (GlobeNewswire) New offering leverages powerful lexical engine and ML models to provide compliance departments with better...

Find MORE on our website.

Technologies, Techniques, and Standards

Cloud misconfigurations and security: 5 ways to avoid your next fail (TechBeacon) Here's how to securely configure your cloud services and keep them safe.

HITRUST Releases Version 9.4 of the HITRUST CSF Incorporating the DoD CMMC, and Approach to Community Standards (HITRUST) Latest release of the HITRUST CSF furthers benefits towards One Framework, One Assessment, Globally™

Forcepoint Makes the Case for the Future of Cloud-Powered Cybersecurity (TechSpective) Forcepoint is hosting the SASE CyberSummit today. SASE is an acronym for Secure Access Service Edge—essentially...

Find MORE on our website.

Design and Innovation

The US Intel Community Is Being Disrupted (Defense One) Intelligence agencies aren't businesses, but they'd better learn from private-sector giants gone by.

Korean IT firms employ AI to maintain decorum in cyberspace (Pulse) The Korean IT names have employed artificial intelligence (AI) programs to oversee decorum in online...

Academia

Illinois Cyber Security Scholars Program (ICSSP) (University of Illinois) The Information Trust Institute (ITI) at the University of Illinois at Urbana-Champaign is an interdisciplinary...

Legislation, Policy, and Regulation

European Authorities Aim to Make National Coronavirus Apps Work Across Borders (Wall Street Journal) The European Union is rushing to figure out how it can make national coronavirus contact-tracing apps...

The Fait Accompli and Persistent Engagement in Cyberspace (War on the Rocks) The Democratic People's Republic of Korea has illicitly generated $2 billion to upgrade its weapons of...

China Hits Back At Cyberattack Claims (Channel News) China is expected to come down heavily on Australian exports as tensions heat up over claims it was responsible...

Find MORE on our website.

Litigation, Investigation, and Law Enforcement

Germany Can Enforce Facebook Data Collection Order (Law360) Germany's high court has dealt Facebook a blow in a landmark case that connects privacy and antitrust...

Full 9th Circ. Won't Reconsider Facebook Wiretap Ruling (Law360) The full Ninth Circuit on Tuesday shot down Facebook's request to reconsider a panel's ruling that users...

Probes Done, No Rulings In Irish Facebook, WhatsApp Cases (Law360) Ireland's data protection watchdog said Tuesday that it had finished probes into both Facebook and its...

Find MORE on our website.

INDUSTRY EVENTS

For a complete running list of events, please visit the Event Tracker on the CyberWire website.

Upcoming Events

WSIS Forum 2020 (Online, June 22 - September 10, 2020) The World Summit on the Information Society (WSIS) Forum 2020, celebrates 15 years of providing a multi-stakeholder...

Hardware Hacking Virtual Conference (Online, June 24, 2020) Join the ioXt Alliance and register now for our upcoming Summer Virtual Conference. You'll hear the latest...

Protecting Your Digital Reality (Online, June 24, 2020) The COVID-19 pandemic has heightened the cybersecurity risks for everyone, including large companies,...

Texas Cyber June'gle Virtual Summit (Online, June 27 - 28, 2020) The Texas Cyber June'gle Virtual Summit is June 27th and June 28th, it runs approximately 30 hours straight,...

FutureCon Virtual Eastern Conference (Online, June 30, 2020) This virtual event features thought-provoking presentations by Industry Security Leaders, esteemed Keynote...

SPONSOR & SUPPORT

Grow your brand and reach new customers.

Grow your brand and increase your customer base by educating our audience about your products, services, and events by advertising on The CyberWire. We've built trust with an influential (and often hard to reach) audience of CISOs, CSOs, and other senior execs in the security space, across a wide array of industry verticals. Learn more.





Copyright © 2020, CyberWire Inc. Views and assertions of the various sources cited, Selected Reading articles, and cartoons are those of the authors and artists, not the CyberWire, Inc.

This email was sent to Keith.Morrison@cookcountyil.gov
why did I get this? | unsubscribe | update subscription preferences

The CyberWire · 8110 Maple Lawn Blvd. · Suite 200 · Fulton, Md 20759 · USA

RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

From:	Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
To:	Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>, Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent:	June 24, 2020 12:33:01 PM CDT
Received:	June 24, 2020 12:33:04 PM CDT
Attachments:	RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

See attached from the data breach

From: Jonathan Springborn (Sheriff)
Sent: Tuesday, June 23, 2020 4:28 PM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: FW: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER
Importance: High

FYI,

You may want to check out this alert and URL.

Data breach affected: Illinois Crime Reporting and Information - Metro East

https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>
Sent: Tuesday, June 23, 2020 11:04 AM
To: Michael Aliperti <Michael.Aliperti@cisecurity.org>; Ben Spear <Ben.Spear@cisecurity.org>
Subject: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

TLP: AMBER

TO: All MS-ISAC Members and Partners

DATE: June 23, 2020

SUBJECT: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach

On June 19, 2020, a Twitter account announced the leak of 10 years of data from police departments, fusion centers, and other law enforcement-related entities currently being tracked on social media as #BlueLeaks. According to the National Fusion Center Association (NFCA), the leak is the result of a compromise at a third party web hosting company, Netsential.

The Twitter account is associated with Distributed Denial of Secrets (DDOS), a collective known for posting leaked or exfiltrated data. The post included a link to a Dark Web location hosting 269GB of files and emails including bulletins, advisories, and guides.

Upon receiving notification of this data breach, the MS-ISAC has confirmed the existence of the dataset and is currently working to analyze the specific contents of the data along with our federal, state, and local partners. At this time, some MS-ISAC products and correspondence have been identified in the leaked data due to the nature of our relationship with fusion centers and law enforcement entities. It is likely that cyber threat actors will utilize MS-ISAC information and/or other portions of the data dump to create tailored phishing campaigns or conduct other malicious cyber activity.

Recommendations:

- Be vigilant for new waves of phishing campaigns spoofing emails or products.
- Implement Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-Based Message Authentication Reporting and Conformance (DMARC), which will assist in ensuring that senders are unable to spoof your email domain. For assistance in implementing these controls, see the Global Cyber Alliance's DMARC Guide https://dmarcguide.globalcyberalliance.org/#/.
- Ensure anti-virus software is up to date.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

The MS-ISAC continues to monitor this situation closely and will release further information as appropriate.

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722



TLP: AMBER

Limited Disclosure, restricted to participants' organizations. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.

Sorry Late Again!

From:	Keith Morrison (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D2EBEC5431A14B10A53942341DBD54F4-KEITH MORRI>
To:	Donna Fitzpatrick (Sheriff) <Donna.Fitzpatrick@cookcountyil.gov>
Sent:	June 24, 2020 12:41:31 PM CDT
Received:	June 24, 2020 12:41:00 PM CDT
Attachments:	David Gray.xlsx, Patrick Kelly.xlsx, Betty Harris.xlsx, John Witulski.xlsx, Jonathan Springborn.xlsx

Keith Morrison
Chief Information Security Officer
Cook County Sheriff's Office
Bureau of Information and Technology
Cook County Sheriff's Office
(773) 674-8117

RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>, Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent: June 24, 2020 12:41:43 PM CDT
Received: June 24, 2020 12:41:32 PM CDT

Perfect!

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Wednesday, June 24, 2020 12:33 PM
To: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

See attached from the data breach

From: Jonathan Springborn (Sheriff)
Sent: Tuesday, June 23, 2020 4:28 PM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: FW: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER
Importance: High

FYI,

You may want to check out this alert and URL.

Data breach affected: Illinois Crime Reporting and Information - Metro East

https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>
Sent: Tuesday, June 23, 2020 11:04 AM
To: Michael Aliperti <Michael.Aliperti@cisecurity.org>; Ben Spear <Ben.Spear@cisecurity.org>
Subject: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

TLP: AMBER

TO: All MS-ISAC Members and Partners

DATE: June 23, 2020

SUBJECT: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach

On June 19, 2020, a Twitter account announced the leak of 10 years of data from police departments, fusion centers, and other law enforcement-related entities currently being tracked on social media as #BlueLeaks. According to the National Fusion Center Association (NFCA), the leak is the result of a compromise at a third party web hosting company, Netsential.

The Twitter account is associated with Distributed Denial of Secrets (DDOS), a collective known for posting leaked or exfiltrated data. The post included a link to a Dark Web location hosting 269GB of files and emails including bulletins, advisories, and guides.

Upon receiving notification of this data breach, the MS-ISAC has confirmed the existence of the dataset and is currently working to analyze the specific contents of the data along with our federal, state, and local partners. At this time, some MS-ISAC products and correspondence have been identified in the leaked data due to the nature of our relationship with fusion centers and law enforcement entities. It is likely that cyber threat actors will utilize MS-ISAC information and/or other portions of the data dump to create tailored phishing campaigns or conduct other malicious cyber activity.

Recommendations:

- Be vigilant for new waves of phishing campaigns spoofing emails or products.
- Implement Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-Based Message Authentication Reporting and Conformance (DMARC), which will assist in ensuring that senders are unable to spoof your email domain. For assistance in implementing these controls, see the Global Cyber Alliance's DMARC Guide https://dmarcguide.globalcyberalliance.org/#/.
- Ensure anti-virus software is up to date.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

The MS-ISAC continues to monitor this situation closely and will release further information as appropriate.

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722



TLP: AMBER

Limited Disclosure, restricted to participants' organizations. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who

need to know the information to protect themselves or prevent further harm.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.

RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

To:	Keith Morrison (Sheriff), Jonathan Springborn (Sheriff), Christopher Moore (Sheriff)
Sent:	June 24, 2020 12:41:43 PM CDT
Received:	June 24, 2020 12:41:32 PM CDT

FYI

From:	Keith Morrison (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D2EBEC5431A14B10A53942341DBD54F4-KEITH MORRI>
To:	CCSO Intel (Sheriff) <CCSO.INTEL@cookcountyil.gov>
Sent:	June 24, 2020 12:43:14 PM CDT
Received:	June 24, 2020 12:43:00 PM CDT

Just a FYI there was a data leak of officer data down in Houston

https://www.theblaze.com/news/blueleaks-hackers-release-countless-records-on-police-officers-all-searchable-by-badge-number

Additional article here

Keith Morrison
Chief Information Security Officer
Cook County Sheriff's Office
Bureau of Information and Technology
Cook County Sheriff's Office
(773) 674-8117

FW: FYI

To:	Sheriff Intel
Sent:	June 24, 2020 12:43:15 PM CDT
Received:	June 24, 2020 12:43:18 PM CDT

FW: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

To: Michael.Tomasiello (Chicago Police) <Michael.Tomasiello@chicagopolice.org>
Sent: June 24, 2020 12:45:16 PM CDT
Received: June 24, 2020 12:45:12 PM CDT

I hope all is well with you and yours… You free for a quick call?

773-674-8117

From: Amar Patel (Sheriff)
Sent: Tuesday, June 23, 2020 8:53 PM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Cc: Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>; Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: Re: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Hi Keith,

Is our Azure data center affiliated with Netsential? I would think not, but can we verify. Can you also see if CPD (CPIC) was included in the leak? Intel works with them with reports and officer safety bulletins. I think they host internally or on AWS, but not sure. Thanks sir.

Thanks,

Amar Patel

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 7:10 AM
Cc: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>; Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

This is a different article from the International Association of Chiefs of Police that relates Netsentinal is a Houston service provider for Law Enforcement.

https://www.theblaze.com/news/blueleaks-hackers-release-countless-records-on-police-officers-all-searchable-by-badge-number

I think our only risk from doxing would be workforce. I pulled the attached reports last Friday and provided them to Chuck at Homeland for review.

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

From:	Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>
To:	Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>, Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent:	June 24, 2020 12:47:12 PM CDT
Received:	June 24, 2020 12:47:12 PM CDT

That's great. If Chuck and his team didn't realize that stuff about Workforce, they do now!

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Wednesday, June 24, 2020 12:33 PM
To: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

See attached from the data breach

From: Jonathan Springborn (Sheriff)
Sent: Tuesday, June 23, 2020 4:28 PM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: FW: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER
Importance: High

FYI,

You may want to check out this alert and URL.

> Data breach affected: Illinois Crime Reporting and Information - Metro East

https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>
Sent: Tuesday, June 23, 2020 11:04 AM
To: Michael Aliperti <Michael.Aliperti@cisecurity.org>; Ben Spear <Ben.Spear@cisecurity.org>
Subject: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

TLP: AMBER

TO: All MS-ISAC Members and Partners

DATE: June 23, 2020

SUBJECT: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach

On June 19, 2020, a Twitter account announced the leak of 10 years of data from police departments, fusion centers, and other law enforcement-related entities currently being tracked on social media as #BlueLeaks. According to the National Fusion Center Association (NFCA), the leak is the result of a compromise at a third party web hosting company, Netsential.

The Twitter account is associated with Distributed Denial of Secrets (DDOS), a collective known for posting leaked or exfiltrated data. The post included a link to a Dark Web location hosting 269GB of files and emails including bulletins, advisories, and guides.

Upon receiving notification of this data breach, the MS-ISAC has confirmed the existence of the dataset and is currently working to analyze the specific contents of the data along with our federal, state, and local partners. At this time, some MS-ISAC products and correspondence have been identified in the leaked data due to the nature of our relationship with fusion centers and law enforcement entities. It is likely that cyber threat actors will utilize MS-ISAC information and/or other portions of the data dump to create tailored phishing campaigns or conduct other malicious cyber activity.

Recommendations:

- Be vigilant for new waves of phishing campaigns spoofing emails or products.
- Implement Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-Based Message Authentication Reporting and Conformance (DMARC), which will assist in ensuring that senders are unable to spoof your email domain. For assistance in implementing these controls, see the Global Cyber Alliance's DMARC Guide https://dmarcguide.globalcyberalliance.org/#/.
- Ensure anti-virus software is up to date.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

The MS-ISAC continues to monitor this situation closely and will release further information as appropriate.

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

MS-ISAC® Elections Infrastructure ISAC

TLP: AMBER

Limited Disclosure, restricted to participants' organizations. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.

RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

From: Patrick Kelly (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=873FFD393E8C44B79E707E6A1056650A-PATRICK KEL>
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>, Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent: June 24, 2020 12:47:12 PM CDT
Received: June 24, 2020 12:47:00 PM CDT

That's great. If Chuck and his team didn't realize that stuff about Workforce, they do now!

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Wednesday, June 24, 2020 12:33 PM
To: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

See attached from the data breach

From: Jonathan Springborn (Sheriff)
Sent: Tuesday, June 23, 2020 4:28 PM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: FW: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER
Importance: High

FYI,

You may want to check out this alert and URL.

Data breach affected: Illinois Crime Reporting and Information - Metro East

https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>
Sent: Tuesday, June 23, 2020 11:04 AM
To: Michael Aliperti <Michael.Aliperti@cisecurity.org>; Ben Spear <Ben.Spear@cisecurity.org>
Subject: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

TLP: AMBER

TO: All MS-ISAC Members and Partners

DATE: June 23, 2020

SUBJECT: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach

On June 19, 2020, a Twitter account announced the leak of 10 years of data from police departments, fusion centers, and other law enforcement-related entities currently being tracked on social media as #BlueLeaks. According to the National Fusion Center Association (NFCA), the leak is the result of a compromise at a third party web hosting company, Netsential.

The Twitter account is associated with Distributed Denial of Secrets (DDOS), a collective known for posting leaked or exfiltrated data. The post included a link to a Dark Web location hosting 269GB of files and emails including bulletins, advisories, and guides.

Upon receiving notification of this data breach, the MS-ISAC has confirmed the existence of the dataset and is currently working to analyze the specific contents of the data along with our federal, state, and local partners. At this time, some MS-ISAC products and correspondence have been identified in the leaked data due to the nature of our relationship with fusion centers and law enforcement entities. It is likely that cyber threat actors will utilize MS-ISAC information and/or other portions of the data dump to create tailored phishing campaigns or conduct other malicious cyber activity.

Recommendations:

- Be vigilant for new waves of phishing campaigns spoofing emails or products.
- Implement Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-Based Message Authentication Reporting and Conformance (DMARC), which will assist in ensuring that senders are unable to spoof your email domain. For assistance in implementing these controls, see the Global Cyber Alliance's DMARC Guide https://dmarcguide.globalcyberalliance.org/#/.
- Ensure anti-virus software is up to date.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

The MS-ISAC continues to monitor this situation closely and will release further information as appropriate.

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

MS-ISAC® Elections Infrastructure ISAC

TLP: AMBER

Limited Disclosure, restricted to participants' organizations. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.

RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

To:	Keith Morrison (Sheriff), Jonathan Springborn (Sheriff), Christopher Moore (Sheriff)
Sent:	June 24, 2020 12:47:12 PM CDT
Received:	June 24, 2020 12:47:00 PM CDT

FW: FYI

From: Amar Patel (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=1214EEE73F204F47A1BAE37F472A2011-AMAR PATEL>
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Sent: June 24, 2020 12:51:13 PM CDT
Received: June 24, 2020 12:51:00 PM CDT

[redacted]

From: CCSO Intel (Sheriff) <CCSO.INTEL@cookcountyil.gov>
Sent: Wednesday, June 24, 2020 12:43 PM
To: Sheriff Intel <sheriff.intel@cookcountyil.gov>
Subject: FW: FYI

From: Keith Morrison (Sheriff)
Sent: Wednesday, June 24, 2020 12:43:14 PM (UTC-06:00) Central Time (US & Canada)
To: CCSO Intel (Sheriff)
Subject: FYI

Just a FYI there was a data leak of officer data down in Houston

https://www.theblaze.com/news/blueleaks-hackers-release-countless-records-on-police-officers-all-searchable-by-badge-number

Additional article here

Keith Morrison
Chief Information Security Officer
Cook County Sheriff's Office
Bureau of Information and Technology
Cook County Sheriff's Office
(773) 674-8117

FW: FYI

To:	Douglas Maclean (Sheriff), Keith Morrison (Sheriff), Leo Schmitz (Sheriff), Bradley Curry (Sheriff), Marlon Parks (Sheriff), Brian White (Sheriff), Arunas Buntinas (Sheriff), Tarry Williams (Sheriff)
Cc:	Adnan Memon (Sheriff), Douglas Maclean (Sheriff)
Sent:	June 24, 2020 12:51:13 PM CDT
Received:	June 24, 2020 12:51:00 PM CDT

RE: FYI

From: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>
Sent: June 24, 2020 12:54:42 PM CDT
Received: June 24, 2020 12:54:43 PM CDT

Yes sir.

From: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>
Sent: Wednesday, June 24, 2020 12:51 PM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: FW: FYI

[redacted]

From: CCSO Intel (Sheriff) <CCSO.INTEL@cookcountyil.gov>
Sent: Wednesday, June 24, 2020 12:43 PM
To: Sheriff Intel <sheriff.intel@cookcountyil.gov>
Subject: FW: FYI

From: Keith Morrison (Sheriff)
Sent: Wednesday, June 24, 2020 12:43:14 PM (UTC-06:00) Central Time (US & Canada)
To: CCSO Intel (Sheriff)
Subject: FYI

Just a FYI there was a data leak of officer data down in Houston

https://www.theblaze.com/news/blueleaks-hackers-release-countless-records-on-police-officers-all-searchable-by-badge-number

Additional article here

Keith Morrison
Chief Information Security Officer
Cook County Sheriff's Office
Bureau of Information and Technology
Cook County Sheriff's Office
(773) 674-8117

RE: FYI

From: Douglas Maclean (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=20EA5411E8A349589C43587009EDD10F-DOUGLAS MAC>
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>
Sent: June 24, 2020 12:54:42 PM CDT
Received: June 24, 2020 12:54:00 PM CDT

Yes sir.

From: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>
Sent: Wednesday, June 24, 2020 12:51 PM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: FW: FYI

[redacted]

From: CCSO Intel (Sheriff) <CCSO.INTEL@cookcountyil.gov>
Sent: Wednesday, June 24, 2020 12:43 PM
To: Sheriff Intel <sheriff.intel@cookcountyil.gov>
Subject: FW: FYI

From: Keith Morrison (Sheriff)
Sent: Wednesday, June 24, 2020 12:43:14 PM (UTC-06:00) Central Time (US & Canada)
To: CCSO Intel (Sheriff)
Subject: FYI

Just a FYI there was a data leak of officer data down in Houston

https://www.theblaze.com/news/blueleaks-hackers-release-countless-records-on-police-officers-all-searchable-by-badge-number

Additional article here

Keith Morrison
Chief Information Security Officer
Cook County Sheriff's Office
Bureau of Information and Technology
Cook County Sheriff's Office
(773) 674-8117

RE: FYI

To: Amar Patel (Sheriff), Keith Morrison (Sheriff), Adnan Memon (Sheriff)
Sent: June 24, 2020 12:54:42 PM CDT
Received: June 24, 2020 12:54:00 PM CDT

FW: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

From: Keith Morrison (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D2EBEC5431A14B10A53942341DBD54F4-KEITH MORRI>
To: Michael.Tomasiello (Chicago Police) <Michael.Tomasiello@chicagopolice.org>
Sent: June 24, 2020 1:16:00 PM CDT
Received: June 24, 2020 1:15:00 PM CDT

I hope all is well with you and yours… You free for a quick call?

773-674-8117

From: Amar Patel (Sheriff)
Sent: Tuesday, June 23, 2020 8:53 PM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Cc: Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>; Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: Re: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Hi Keith,

Is our Azure data center affiliated with Netsential? I would think not, but can we verify. Can you also see if CPD (CPIC) was included in the leak? Intel works with them with reports and officer safety bulletins. I think they host internally or on AWS, but not sure. Thanks sir.

Thanks,

Amar Patel

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 7:10 AM
Cc: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>; Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

This is a different article from the International Association of Chiefs of Police that relates Netsentinal is a Houston service provider for Law Enforcement.

https://www.theblaze.com/news/blueleaks-hackers-release-countless-records-on-police-officers-all-searchable-by-badge-number

I think our only risk from doxing would be workforce. I pulled the attached reports last Friday and provided them to Chuck at Homeland for review.

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff)

<Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

No Action Needed

From: Wing, Gregory J. (CG) (FBI) <gjwing@fbi.gov>
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: June 24, 2020 1:52:02 PM CDT
Received: June 24, 2020 1:52:09 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

10-4. Thanks

On Jun 24, 2020 1:50 PM, "Keith Morrison (Sheriff)" <Keith.Morrison@cookcountyil.gov> wrote:
I hope all is well with you and yours

I am sure you already know this….

A contractor for a bunch of police agencies was hacked and their data posted down in Houston…

https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

he worked with some of your guys down there

https://archives.fbi.gov/archives/about-us/partnerships_and_outreach/community_outreach/dcla/2011/houston-1

RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

From: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>, Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent: June 24, 2020 2:02:23 PM CDT
Received: June 24, 2020 2:02:24 PM CDT

Awesome!

Glad our data was not leaked.

Springborn

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Wednesday, June 24, 2020 12:33 PM
To: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

See attached from the data breach

From: Jonathan Springborn (Sheriff)
Sent: Tuesday, June 23, 2020 4:28 PM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: FW: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER
Importance: High

FYI,

You may want to check out this alert and URL.

Data breach affected: Illinois Crime Reporting and Information - Metro East

https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>
Sent: Tuesday, June 23, 2020 11:04 AM
To: Michael Aliperti <Michael.Aliperti@cisecurity.org>; Ben Spear <Ben.Spear@cisecurity.org>
Subject: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

TLP: AMBER

TO: All MS-ISAC Members and Partners

DATE: June 23, 2020

SUBJECT: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach

On June 19, 2020, a Twitter account announced the leak of 10 years of data from police departments, fusion centers, and other law enforcement-related entities currently being tracked on social media as #BlueLeaks. According to the National Fusion Center Association (NFCA), the leak is the result of a compromise at a third party web hosting company, Netsential.

The Twitter account is associated with Distributed Denial of Secrets (DDOS), a collective known for posting leaked or exfiltrated data. The post included a link to a Dark Web location hosting 269GB of files and emails including bulletins, advisories, and guides.

Upon receiving notification of this data breach, the MS-ISAC has confirmed the existence of the dataset and is currently working to analyze the specific contents of the data along with our federal, state, and local partners. At this time, some MS-ISAC products and correspondence have been identified in the leaked data due to the nature of our relationship with fusion centers and law enforcement entities. It is likely that cyber threat actors will utilize MS-ISAC information and/or other portions of the data dump to create tailored phishing campaigns or conduct other malicious cyber activity.

Recommendations:

- Be vigilant for new waves of phishing campaigns spoofing emails or products.
- Implement Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-Based Message Authentication Reporting and Conformance (DMARC), which will assist in ensuring that senders are unable to spoof your email domain. For assistance in implementing these controls, see the Global Cyber Alliance's DMARC Guide https://dmarcguide.globalcyberalliance.org/#/.
- Ensure anti-virus software is up to date.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

The MS-ISAC continues to monitor this situation closely and will release further information as appropriate.

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

TLP: AMBER

Limited Disclosure, restricted to participants' organizations. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.

RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

From: Jonathan Springborn (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=32F2A0A9AA124C638CA1784E3422B464-JONATHAN SP>
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>, Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent: June 24, 2020 2:02:23 PM CDT
Received: June 24, 2020 2:02:00 PM CDT

Awesome!

Glad our data was not leaked.

Springborn

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Wednesday, June 24, 2020 12:33 PM
To: Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: RE: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

See attached from the data breach

From: Jonathan Springborn (Sheriff)
Sent: Tuesday, June 23, 2020 4:28 PM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>; Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Subject: FW: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER
Importance: High

FYI,

You may want to check out this alert and URL.

Data breach affected: Illinois Crime Reporting and Information - Metro East

https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/

Jonathan Springborn
Jonathan.Springborn@cookcountyil.gov
(773)674-6850 – Helpdesk
(773)674-7762 – Office Desk Phone

From: MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>
Sent: Tuesday, June 23, 2020 11:04 AM
To: Michael Aliperti <Michael.Aliperti@cisecurity.org>; Ben Spear <Ben.Spear@cisecurity.org>
Subject: Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

TLP: AMBER

TO: All MS-ISAC Members and Partners

DATE: June 23, 2020

SUBJECT: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach

On June 19, 2020, a Twitter account announced the leak of 10 years of data from police departments, fusion centers, and other law enforcement-related entities currently being tracked on social media as #BlueLeaks. According to the National Fusion Center Association (NFCA), the leak is the result of a compromise at a third party web hosting company, Netsential.

The Twitter account is associated with Distributed Denial of Secrets (DDOS), a collective known for posting leaked or exfiltrated data. The post included a link to a Dark Web location hosting 269GB of files and emails including bulletins, advisories, and guides.

Upon receiving notification of this data breach, the MS-ISAC has confirmed the existence of the dataset and is currently working to analyze the specific contents of the data along with our federal, state, and local partners. At this time, some MS-ISAC products and correspondence have been identified in the leaked data due to the nature of our relationship with fusion centers and law enforcement entities. It is likely that cyber threat actors will utilize MS-ISAC information and/or other portions of the data dump to create tailored phishing campaigns or conduct other malicious cyber activity.

Recommendations:

- Be vigilant for new waves of phishing campaigns spoofing emails or products.
- Implement Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-Based Message Authentication Reporting and Conformance (DMARC), which will assist in ensuring that senders are unable to spoof your email domain. For assistance in implementing these controls, see the Global Cyber Alliance's DMARC Guide https://dmarcguide.globalcyberalliance.org/#/.
- Ensure anti-virus software is up to date.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

The MS-ISAC continues to monitor this situation closely and will release further information as appropriate.

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722



TLP: AMBER

Limited Disclosure, restricted to participants' organizations. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.

RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

To:	Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>
Cc:	Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>, Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>, Michael.Tomasiello (Chicago Police) <Michael.Tomasiello@chicagopolice.org>
Received:	June 24, 2020 2:24:57 PM CDT
Attachments:	image001.png, domains they own.txt

From the best I can tell digging into their supply chain they are a Microsoft shop not AWS.

Supply Chain

Netsential.Com (netsential.com) Business Data Customer Data 3 M

Category / Vendor	Main Website
Widgets (1)	
Webserver (2)	
Microsoft	microsoft.com
Microsoft IIS	iis.net
Webmaster tools (1)	
Google	google.com

Their website relates they are working with LE at the moment.
The owner was
I contacted Tomasiello at CPD waiting for a response from him.

From: Amar Patel (Sheriff)
Sent: Tuesday, June 23, 2020 8:53 PM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Cc: Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>; Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: Re: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Hi Keith,

Is our Azure data center affiliated with Netsential? I would think not, but can we verify. Can you also see if CPD (CPIC) was included in the leak? Intel works with them with reports and officer safety bulletins. I think they host internally or on AWS, but not sure. Thanks sir.

Thanks,

Amar Patel

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 7:10 AM
Cc: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>; Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

This is a different article from the International Association of Chiefs of Police that relates Netsentinal is a Houston service provider for Law Enforcement.

https://www.theblaze.com/news/blueleaks-hackers-release-countless-records-on-police-officers-all-searchable-by-badge-number

I think our only risk from doxing would be workforce. I pulled the attached reports last Friday and provided them to Chuck at Homeland for review.

From: Keith Morrison (Sheriff)
Sent: Tuesday, June 23, 2020 6:45 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

[redacted]

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:26 AM
To: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Keith –

[redacted]

Doug

From: Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent: Tuesday, June 23, 2020 6:20 AM
To: Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>; Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Deputy CIO Maclean,

[redacted]

Thanks,

Morrison

From: Douglas Maclean (Sheriff)
Sent: Tuesday, June 23, 2020 6:10 AM
To: Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>; Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>; Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>
Subject: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

Krebs on Security reports Blue Leaks has posted 24 years of LEA and fusion center-related data as the result of a breach on Netsential, an internet services provider to LEAs and operational fusion centers. The data includes some information related to sensitive operations and a significant amount of PII.

The Krebs on Security story can be found here

Keith – do we have any exposure from this breach either directly from our own infrastructure or indirectly as the result of data-sharing with other agencies? Do any of our vendors use or have they used Netsential for any of their operations from 1994 to present?

Douglas MacLean
Deputy CIO
Cook County Sheriff's Office
3026 S. California
South Campus Building 1
Chicago IL 60608
312.877.2048 [c]
773.674.8615 [d]

RE: IMPORTANT: Blue Leaks Posts 24 Years of Fusion Center Data

From:	Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
To:	Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>
Cc:	Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>, Douglas Maclean (Sheriff) <Douglas.Maclean2@cookcountyil.gov>
Sent:	June 24, 2020 2:28:43 PM CDT
Received:	June 24, 2020 2:28:43 PM CDT
Attachments:	domains they own.txt

From the best I can tell digging into their supply chain they are a Microsoft shop not AWS.

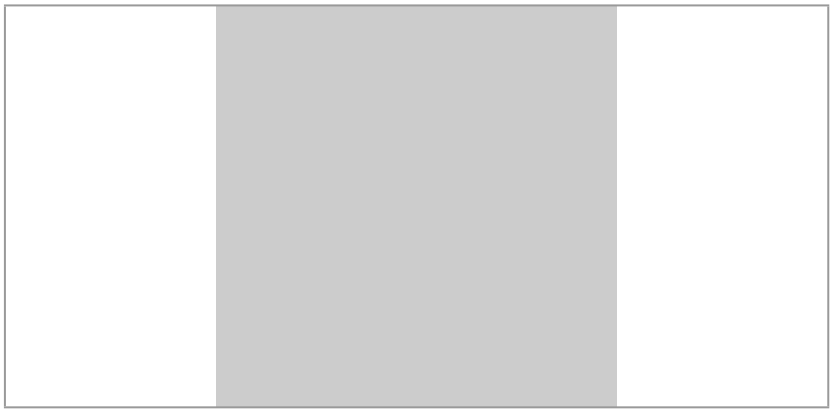
Threat Actor Sold Access to Networks of 135 Organizations:

From:	SecurityWeek Briefing <news@securityweek.com>
To:	jonathan.springborn@cookcountyil.gov, Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>
Sender:	SecurityWeek Briefing <news@securityweek.ccsend.com>
Sent:	June 24, 2020 3:23:27 PM CDT
Received:	June 24, 2020 3:23:31 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Wednesday, June 24, 2020



Sodinokibi Ransomware Operators Target POS Software: The threat actor behind the Sodinokibi ransomware was observed scanning the victim networks for credit card or point of sale (POS) software. **Read More**

Threat Actor Sold Access to Networks of 135 Organizations: Over a period of two years, a threat actor sold access to the compromised networks of 135 organizations in 44 countries and likely made over $1.5 million. **Read More**

VMware Patches Several Vulnerabilities Allowing Code Execution on Hypervisor: VMware addresses

Why Does Asset Management Matter for Cybersecurity?

Download the free white paper today to learn why modern asset management is the nexus for cybersecurity projects and decisions.

Read Now

Defending Your Budget: How to Show ROI of Cybersecurity Investments

Developing an ROI model takes time ñ my recommendation would be to focus on a simple security project that will return high value to the business when proven successful.
Read the Full Column by **Laurence Pitt**

Non-Human Identities: The New Blindspot in Cybersecurity

The integration of identity with security is still work in progress, with less than half of businesses having fully implemented key identity-related access controls according to a research study.
Read the Full Column by **Torsten George**

New Reality of IT-OT: Convergence, Collaboration and Digital Transformation Acceleration

Itís very challenging for OT professionals to play catch up and close the 25+ year IT-OT security gap, particularly as the number of connectivity points grows exponentially.
Read the Full Column by **Galina Antova**

To Err Is Human: Accepting Responsibility to Regain Confidence

Regardless of what goes wrong, the right attitude goes a long way towards helping stakeholders regain confidence in the security team and the security program it is running.
Read the Full Column by **Joshua Goldfarb**

Navigating the Rapid Digital Shift: Ticket on the Bus, Not the Whole Bus

With a diverse and globally distributed workforce, cybersecurity buying decisions will increasingly factor accessibility, usability, and inclusiveness in solution design and operability.
Read the Full Column by **Gunter Ollmann**

SD-WAN Must Be Secure, Flexible, and Scale Across the Entire Enterprise

Smart businesses are learning that SD-WAN can play a critical role in quicklyóand securelyórolling out new networking environments, and

10 vulnerabilities in ESXi, Workstation and Fusion products, including serious flaws that can be exploited for code execution on the hypervisor. **Read More**

Dridex Operators Develop 'WastedLocker' Ransomware: The threat actor behind the Dridex Trojan has released a new ransomware following months of development. **Read More**

Bug Hunters Confident They Will Continue to Outperform AI: Study: Hackers are confident that they will outperform AI for the next 10 years when it comes to finding vulnerabilities, Bugcrowd study shows. **Read More**

Senators Introduce "Balanced" Bill That Aims to End Warrant-Proof Encryption: Republican senators have introduced what they have described as a ìbalancedî bill that would require tech companies to give law enforcement access to encrypted data.**Read More**

Companies Say Strong Authentication Important But Still Over-Rely on Passwords: Companies believe strong authentication is important, but they still over-rely on passwords and allow their employees to access corporate resources via social media credentials. **Read More**

Twitter Suspends Account of Organization Behind Police Leaks: Twitter has suspended the account of Distributed Denial of Secrets after it posted links to information on 200 law enforcement organizations. **Read More**

German Court Orders Facebook to Rein in Data Collection: A top German court has ordered Facebook to stop merging data collected through its Whatsapp and Instagram subsidiaries or other websites unless users explicitly agree, in a legal victory for competition authorities. **Read More**

Microsoft Chief Says EU 'Most Influential' on Tech Rules: Microsoft president Brad Smith on Tuesday said Europe was the global leader on setting rules for big tech, two years after the EU implemented the GDPR, its landmark data privacy law. **Read More**

Safe Documents Feature in Microsoft 365 Apps Now Generally Available: Microsoft this week announced that Safe Documents, a feature meant to boost the protection of Microsoft 365 users when opening unsafe documents, is generally available. **Read More**

COVID-19 Fuels Phishing and Scams While BEC Attacks Evolve and Increase: COVID-19 is fueling phishing and scams while BEC attacks continue to evolve and increase, according to a report from Abnormal Security. **Read More**

Twitter Alerts Business Users of Billing Information Exposure: Twitter has informed business users that their billing information may have been exposed through their web browserís cache. **Read More**

Micro-Segmentation for Endpoints Shows Promising Defense Against Lateral Movement: Applying micro-segmentation to endpoints can help

connecting resources and users to data and applications.
[Read the Full Column] by **John Maddison**

Strengthen Cybersecurity With These 3 Steps to Rapid Response

With capabilities to quickly curate and integrate new threat data sources across your operations, youíre prepared for whatever the future brings.
[Read the Full Column] by **Marc Solomon**

3 Ways Effective OT Security Enables Your Business

When your core business operations, digital transformation initiatives and workersí ability to do their jobs are at risk, effective OT security must become just as ubiquitous.
[Read the Full Column] by **Galina Antova**

Realizing the Potential of AI-Driven Security Operations

By combining ML and AI with a team of advanced cybersecurity professionals to deploy true AI-driven security operations, organizations can stay a step ahead of cybercriminals.
[Read the Full Column] by **John Maddison**

Protecting Online Retail in the Face of COVID-19 and Beyond

Every business is likely to be subject to cyberattacks at some point, and the option is to either take on the cost of putting measures in place before it happens or paying to clean up after.
[Read the Full Column] by **Laurence Pitt**

On the Rise: The Enemy From Within

Today's economic climate exacerbates risks of insider threats, as pending furloughs or pay cuts may tempt employees to exfiltrate data to secure a new job, make up for income losses, etc.
[Read the Full Column] by **Torsten George**

Seven Ways to Improve Efficiency in Your Security Metrics Program

Most security organizations realize that, regardless of how much progress they've made towards improving maturity and efficiency, there is still more work to be done.
[Read the Full Column] by **Joshua Goldfarb**

Why You May Not Need to Monitor the Dark Web

Many organizations are steadfast in their belief that dark web monitoring is a critical part of their security operations and the security industry is happy to fuel that belief.
[Read the Full Column] by **Idan Aharoni**

stop attackers from moving laterally within an organization after the initial breach. [Read More]

XORDDoS, Kaiji DDoS Botnets Target Docker Servers: The XORDDoS and Kaiji DDoS botnets have started targeting exposed Docker servers, Trend Micro warns. [Read More]

U.S. Pushes for HTTPS on .gov Domains: The United States is taking additional steps toward serving .gov domains over encrypted connections, and this week laid out plans to preload the entire top-level domain (TLD). [Read More]

Apple Announces New Privacy Features at WWDC 2020: Apple has announced several new privacy and security features at its 2020 Worldwide Developers Conference (WWDC). [Read More]

Mitsubishi Patches Vulnerabilities Disclosed at ICS Hacking Contest: Mitsubishi Electric and its subsidiary ICONICS have released patches for the vulnerabilities disclosed earlier this year at the Pwn2Own hacking competition targeting ICS. [Read More]

N.Zealand Freezes Assets of Alleged Russian Cyber Criminal: New Zealand police has frozen NZ$140 million (US$90 million) in assets linked to a Russian man accused of laundering money for organised crime using cyber currency. [Read More]

Microsoft Acquires Industrial Cybersecurity Company CyberX: Microsoft has acquired industrial cybersecurity company CyberX in an effort to expand its Azure IoT security capabilities and extend them to IIoT and OT. [Read More]

Vulnerability in OSIsoft PI System Can Facilitate Attacks on Critical Infrastructure: A stored XSS vulnerability in OSIsoft PI System, a product often present in critical infrastructure facilities, can be exploited for phishing, privilege escalation and other purposes. [Read More]

Spyware by Israel's NSO Used Against Journalist: Amnesty: Amnesty International says software developed by Israeli security firm NSO Group was used to attack a Moroccan journalist, the latest in a series of allegations against the company. [Read More]

BlueLeaks: Data From Hundreds of Law Enforcement Organizations Leaked Online: BlueLeaks: Distributed Denial of Secrets has leaked hundreds of thousands of files belonging to over 200 law enforcement agencies, obtained by Anonymous hackers from a web development firm. [Read More]

Microsoft Boosts Protections for US AccountGuard Users: Microsoft has announced improved identity and access management protections for AccountGuard users in the United States, ahead of the 2020 elections. [Read More]

AMD Preparing Patches for UEFI SMM Vulnerability: AMD is preparing patches for a vulnerability affecting the System Management Mode (SMM) of the UEFI shipped for some notebook and embedded processors. [Read More]

Data is the Key to Understand Whatever Life Brings

With an extensible platform and flexible data model, you can take full advantage of the volume and variety of data to gain insights, and the technologies in your ecosystem to accelerate detection and response and mitigate risk.
Read the Full Column by **Marc Solomon**

Beware of Sick Behavior Masquerading as Coronavirus

Researchers have undertaken a deep dive into the shadowy, cyber world of those whose work involves abusing others online through trickery, extortion, fraud, and theft resulting from COVID-19.
Read the Full Column by **Alastair Paterson**

Three Tips to Help CISOs Close the IT-OT Security Gap, Part 2

Eliminate complexity, align IT and OT teams, and simplify governance are my top three recommendations for how to bridge the IT-OT security gap.
Read the Full Column by **Galina Antova**

Now That Everyone's Working From Home, How's Your Helpdesk Holding Up?

Heightened anxiety is a normal consequence of drastic change, and it's natural for the entire organization to be stressed by the shift to a fully remote work environment.
Read the Full Column by **Jim Ducharme**

See All Recent Articles at SecurityWeek.Com

U.S. Sanctions Six Nigerians for BEC and Romance Fraud: The U.S. Treasury Department and the Justice Department announce sanctions against six Nigerian nationals for their involvement in BEC and romance fraud schemes. **Read More**

Google Loses Appeal Against 50-Mn-Euro French Fine: France's highest administrative authority on Friday dismissed a challenge by Google against a fine of 50 million euros ($56 million) for failing to provide adequate information on its data consent policies. **Read More**

Tens of Malicious Chrome Extensions Used in Global Surveillance Campaign: Malicious Chrome extensions employed in a massive global surveillance campaign have been downloaded by millions before removal. **Read More**

Flaw in IBM Asset Management Product Facilitates Attacks on Corporate Networks: A high-severity vulnerability found in IBMís Maximo asset management product makes it easier for hackers to move around in enterprise networks. **Read More**

Man Accused of Hacking University of Pittsburgh Medical Center Gets Arrested: The alleged hacker who breached the human resource databases of University of Pittsburgh Medical Center in 2014 was arrested this week in Detroit. **Read More**

Mysterious 'AcidBox' Malware Used Turla Exploit to Target Russian Organizations: Targeted attacks delivering a new piece of malware leveraged an exploit previously associated with the Russian-linked Turla hacking group. **Read More**

To help make sure the SecurityWeek Briefing reaches you, please add news@securityweek.com to your address book.

© 2020 Wired Business Media

Visit SecurityWeek.Com | Twitter | Advertise | Contact

SecurityWeek | 40 Warren Street, Charlestown, MA 02129

Unsubscribe jonathan.springborn@cookcountyil.gov

Update Profile | About Constant Contact

Sent by news@securityweek.com

Tasks

From:	Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>
To:	Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
Sent:	June 24, 2020 10:15:18 PM CDT
Received:	June 24, 2020 10:15:19 PM CDT
Attachments:	WORK_062420.xlsx

Attached.

Jonathan Springborn
Cook County Sheriff's Office
Sheriff's Information Technology Unit
3026 S. California, Chicago, IL 60608
Jonathan.Springborn@cookcounyil.gov
(773) 674-6850 – Sheriff Help Desk
(312) 339-2995 – Mobile
www.cookcountysheriff.org

Tasks

From:	Jonathan Springborn (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=32F2A0A9AA124C638CA1784E3422B464-JONATHAN SP>
To:	Keith Morrison (Keith.Morrison@cookcountyil.gov) <Keith.Morrison@cookcountyil.gov>
Sent:	June 24, 2020 10:15:18 PM CDT
Received:	June 24, 2020 10:15:00 PM CDT
Attachments:	WORK_062420.xlsx

Attached.

Jonathan Springborn
Cook County Sheriff's Office
Sheriff's Information Technology Unit
3026 S. California, Chicago, IL 60608
Jonathan.Springborn@cookcounyil.gov
(773) 674-6850 – Sheriff Help Desk
(312) 339-2995 – Mobile
www.cookcountysheriff.org

Tasks

To:	Keith Morrison (Keith.Morrison@cookcountyil.gov), Keith Morrison (Sheriff), Patrick Kelly (Sheriff), Christopher Moore (Sheriff)
Sent:	June 24, 2020 10:15:18 PM CDT
Received:	June 24, 2020 10:15:00 PM CDT

:-)

From:	Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
To:	Donna Fitzpatrick (Sheriff) <Donna.Fitzpatrick@cookcountyil.gov>
Sent:	June 25, 2020 6:41:34 AM CDT
Received:	June 25, 2020 6:41:37 AM CDT
Attachments:	Jonathan Springborn.xlsx, Betty Harris.xlsx, Patrick Kelly.xlsx, John Witulski.xlsx, David Gray.xlsx

Keith Morrison
Chief Information Security Officer
Cook County Sheriff's Office
Bureau of Information and Technology
Cook County Sheriff's Office
(773) 674-8117

:-)

To:	Donna Fitzpatrick (Sheriff)
Sent:	June 25, 2020 6:41:34 AM CDT
Received:	June 25, 2020 6:41:42 AM CDT

:-)

From:	Keith Morrison (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D2EBEC5431A14B10A53942341DBD54F4-KEITH MORRI>
To:	Donna Fitzpatrick (Sheriff) <Donna.Fitzpatrick@cookcountyil.gov>
Sent:	June 25, 2020 6:41:34 AM CDT
Received:	June 25, 2020 6:41:00 AM CDT
Attachments:	Jonathan Springborn.xlsx, Betty Harris.xlsx, Patrick Kelly.xlsx, John Witulski.xlsx, David Gray.xlsx

Keith Morrison
Chief Information Security Officer
Cook County Sheriff's Office
Bureau of Information and Technology
Cook County Sheriff's Office
(773) 674-8117

IT Security News Blast - 6-25-2020

From: Mike Hamilton <Michael.Hamilton@CI.Security>
To: Keith.Morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: June 25, 2020 7:14:10 AM CDT
Received: June 25, 2020 7:14:22 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

IT Security News Blast – 6-25-2020

Ransomware perspectives: The shape of things to come – Interview with CISO Mike Hamilton

Mike Hamilton, CISO of CI Security, discusses ransomware attacks and offers insight on how to strengthen the cybersecurity program to defend against new TTPs by threat actors. Mike discusses the impacts ransomware attacks have on cities and how properly staffing up on InfoSec talent is critical to managing ransomware risks. “Your monitoring must be comprehensive, and someone must be assigned to follow up and investigate security alerts,” notes Mike. “Without proper people resourcing, your technology is yelling into the wind. Ask Target how this works out.”

https://www.helpnetsecurity.com/2020/06/24/ransomware-perspectives/

New WastedLocker ransomware demands payments of millions of USD

In an interview with ZDNet earlier today, Fox-IT says they've been tracking the use of this new ransomware family since May 2020. They say the ransomware has been exclusively deployed against US companies. "Ransom demands that are asked by

Evil Corp are now typically into the millions," Maarten van Dantzig, Fox-IT security researcher, told ZDNet today. "We've seen demands of more than $10 million," he added. [...] "Typically, they hit file servers, database services, virtual machines, and cloud environments," researchers said.

https://www.zdnet.com/article/new-wastedlocker-ransomware-demands-payments-of-millions-of-usd/

Fxmsp hackers made $1.5M selling access to corporate networks

Fxmsp became widely known outside hacker forums about a year ago when cybersecurity boutique Advanced Intelligence (AdvIntel) published a series of reports on the actor’s attempts to close a $300,000 deal for selling access to networks belonging to Symantec, Trend Micro, and McAfee. [...] According to Yelisey Boguslavskiy, AdvIntel director of security research, Fxmsp was the hacking part of a crew (GPTitan) consisting of specialists "geared to secretly work in financial environments" to steal from high-profile networks data relevant to customers.

https://www.bleepingcomputer.com/news/security/fxmsp-hackers-made-15m-selling-access-to-corporate-networks/

Bungled Lancet study casts shadow over health data industry

The ensuing scandal threw a damper on the idea of medical research being based entirely on big sets of health data, at a time when the market for health data is booming and big industrial players are pushing for its use in medical research. Google this week formally notified the European Commission of its plans to buy wearable health tracking devices company Fitbit — and its troves of sensitive health data — in a deal that has alarmed privacy campaigners, while Palantir, a U.S. data mining company, recently gained access to U.K. health data.

https://www.politico.com/news/2020/06/24/lancet-study-hydroxychloroquine-health-data-industry-337663

3 Key Ways to Bolster Healthcare Cybersecurity with MFA, Training

For the healthcare sector, already burdened with the Coronavirus response, the

expanded threat landscape could lead to some serious issues down the line. Fortunately, the majority of these advisories contain key elements that could allow enterprises to effectively close some of these critical gaps.

- MULTI-FACTOR AUTHENTICATION
- USER EDUCATION, TRAINING
- ASSET INVENTORY AND PATCH MANAGEMENT

https://healthitsecurity.com/news/3-key-ways-to-bolster-healthcare-cybersecurity-with-mfa-training

CISA's Ware Runs Down COVID-19 Cyber Threats to Health Sectors

Despite the massive turn to telework at government agencies and in the private sector during the pandemic – and the accompanying assault of cyber attacks from actors looking to take advantage of the situation – Ware said that CISA has continued on pace with other missions, including effort to secure the national elections in November. He said the "risk picture" for CISA has shown up strongly in four categories: phishing exploit increases; ransomware attacks on healthcare systems; espionage against pharmaceutical companies and laboratories; and risks involved with shift to telework.

https://www.meritalk.com/articles/cisas-ware-runs-down-covid-19-cyber-threats-to-health-sectors/

Indiabulls Group hit by CLOP Ransomware, gets 24h leak deadline

"The Indiabulls Group is a diversified financial services group with interests in housing finance, consumer finance and personal wealth. The Group also has a presence in Real Estate, Pharmaceuticals, Lighting and Infrastructure & Construction Equipment Leasing[.]" [...] Cyberintelligence firm Bad Packets told BleepingComputer, though, that Indiabulls has an Citrix Netscaler ADC VPN gateway exposed, which is vulnerable to the CVE-2019-19781 vulnerability.

https://www.bleepingcomputer.com/news/security/indiabulls-group-hit-by-clop-ransomware-gets-24h-leak-deadline/

FBI, DoJ Officials Warn of Common COVID-19 Cyber Threat Vectors

Tonya Ugoretz, deputy assistant director of the FBI's Cyber Division, reported that the agency's Internet Crime Complaint Center has seen as many complaints as this point in 2020 as they did in all of 2019. Of those complaints, she said at the June 24 Fal.Con for the Public Sector CrowdStrike Cybersecurity Conference, at least 20,000 have been about COVID-19 related schemes.

https://www.meritalk.com/articles/fbi-doj-officials-warn-of-common-covid-19-cyber-threat-vectors/

Banks can ill afford to get complacent about coronavirus

[Cyber] resiliency in a business continuity model is going to be crucial to ensuring a safe and secure financial system. Cyber resiliency is broader than the traditional business continuity focus on data backup and recovery. It's about data integrity and the ability to trust the data to know with confidence that backed-up data has not been corrupted or altered by a cyberattack. Resilience is the ability to operate, even in a degraded state, and recover from deliberate attacks.

https://www.americanbanker.com/opinion/banks-can-ill-afford-to-get-complacent-about-coronavirus

There's No Vaccine For Data Leaks: Why One Cyber Attack Leads To Another

Businesses have become far too accustomed to massive security breaches, disregarding them like the common cold. Often, the remedy appears to be free credit monitoring for the affected. But the real threat is lost in that perception of safety and a healthy bounce-back. Many significant risks are escalated after a breach leveraging the data that is lost in these incidents — stolen personal details enable ransomware or "man-in-the-middle" breaches to be more targeted and effective.

https://www.forbes.com/sites/emilsayegh/2020/06/24/theres-no-vaccine-for-data-leaks-why-one-cyber-attack-leads-to-another/#58d58a757300

Senate wants more clarity on cyber ops

In its version of the annual defense policy bill — which passed the committee last week, though full text of the language was only made public this week — the committee takes aim at U.S. Cyber Command's so-called hunt forward operations. Hunt forward operations involve teams from Cyber Command physically deploying to other nations to assist them with cyber defense. These operations provide American cyber teams insight into tactics that could be turned against U.S. networks or used to disrupt the elections process, officials have maintained.

https://www.fifthdomain.com/congress/2020/06/24/senate-wants-more-clarity-on-cyber-ops/

Cyber attack on Israeli water-treatment plant is one indication of a rising tide of cyber security issues

The water facility attack was to release large amounts of poisonous chlorine into Israel's water delivery infrastructure, potentially poisoning tens of thousands of Israelis. It may indicate a growing threat of cyber attack throughout the world. FireEye, a publicly traded cyber security company in Milpitas, California, determined that the malware developed for this kind of attack came out of Russia and specifically from the Central Scientific Research Institute of Chemistry and Mechanics, a Russian government-owned technical research institution in Moscow.

https://www.militaryaerospace.com/trusted-computing/article/14178333/cyber-security-growing-threat-international-actors

China is Retooling, and Russia Seeks Harm to Critical Infrastructure

China and Russia continue to pose the greatest espionage and cyber attack threats to the United States, but the intelligence leader anticipates that other adversaries and strategic competitors will also build and integrate cyber espionage, cyber attacks and influence operations into how they conduct business. "Our strategic competitors will increasingly use cyber space capabilities including cyber espionage, cyber attack and continued influence operations to seek political, economic and military advantage over the United States, our allies and our partners," he said. "This is not an 'if,' it is a yes. They are doing it and they will continue."

https://www.afcea.org/content/china-retooling-and-russia-seeks-harm-critical-infrastructure

Police arrested wrong man based on facial recognition fail, ACLU says

The American Civil Liberties Union filed the complaint (PDF) Wednesday on behalf of Robert Williams, a Michigan man who was arrested in January based on a false positive generated by facial recognition software. "At every step, DPD's conduct has been improper," the complaint alleges. "It unthinkingly relied on flawed and racist facial recognition technology without taking reasonable measures to verify the information being provided" as part of a "shoddy and incomplete investigation."

https://arstechnica.com/tech-policy/2020/06/police-arrested-wrong-man-based-on-facial-recognition-fail-aclu-says/

Twitter bans DDoSecrets account over 'BlueLeaks' police data dump

On Friday, last week, the group published 296 GB of data they claimed to have received from the Anonymous hacker collective. The data dump, dubbed BlueLeaks, contained millions of documents that were stolen from a Texas company named Netsential that provided web hosting services for various US law enforcement entities. Subsequent analysis revealed that the BlueLeaks data dump contained files from more than 200 US police departments, fusion centers, and other law enforcement training and support portals.

https://www.zdnet.com/article/twitter-bans-ddosecrets-account-over-blueleaks-police-data-dump/

Self-Propagating Lucifer Malware Targets Windows Systems

The never-before-seen malware initially tries to infect PCs by bombarding them with exploits in hopes of taking advantage of an “exhaustive” list of unpatched vulnerabilities. While patches for all the critical and high-severity bugs exist, the various companies impacted by the malware had not applied the fixes. [...] The vulnerabilities targeted by Lucifer include Rejetto HTTP File Server (CVE-2014-6287), Oracle Weblogic (CVE-2017-10271), ThinkPHP RCE (CVE-2018-20062), Apache Struts (CVE-2017-9791), Laravel framework CVE-2019-9081), and

Microsoft Windows (CVE-2017-0144, CVE-2017-0145, and CVE-2017-8464).

https://threatpost.com/self-propagating-lucifer-malware-targets-windows-systems/156883/

Republicans Who Don't Understand Encryption Introduce Bill to Break It

While the senators do name a few instances in which encryption made it harder for the cops to investigate shootings and organized crime, they also chose the well-trodden path of waving their arms and scream about terrorism and protecting children, while blaming tech companies for not doing enough.

https://www.vice.com/en_us/article/y3z3z7/republican-encryption-bill-privacy-signal

You are receiving this email because you are subscribed to receive the IT Security Daily Blast email from Michael Hamilton, Founder, President, and CISO of CI Security, formerly Critical Informatics.

Archived articles are available at https://ci.security/news/daily-news.

CI Security and the CI Security logo are the trademarks of CI Security, Inc. All other brand names, trademarks, service marks, and copyrights are the property of their respective owners.

© 2020 CI Security. All rights reserved.

CI Security

245 4th St, Suite 405 Bremerton, WA 98337

IT Security News Blast - 6-25-2020

From: Mike Hamilton <Michael.Hamilton@CI.Security>
To: christopher.moore@cookcountyil.gov, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>

Sent: June 25, 2020 7:14:10 AM CDT
Received: June 25, 2020 7:14:18 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

IT Security News Blast – 6-25-2020

Ransomware perspectives: The shape of things to come – Interview with CISO Mike Hamilton

Mike Hamilton, CISO of CI Security, discusses ransomware attacks and offers insight on how to strengthen the cybersecurity program to defend against new TTPs by threat actors. Mike discusses the impacts ransomware attacks have on cities and how properly staffing up on InfoSec talent is critical to managing ransomware risks. “Your monitoring must be comprehensive, and someone must be assigned to follow up and investigate security alerts,” notes Mike. “Without proper people resourcing, your technology is yelling into the wind. Ask Target how this works out.”

https://www.helpnetsecurity.com/2020/06/24/ransomware-perspectives/

New WastedLocker ransomware demands payments of millions of USD

In an interview with ZDNet earlier today, Fox-IT says they've been tracking the use of this new ransomware family since May 2020. They say the ransomware has been exclusively deployed against US companies. "Ransom demands that are asked by

Evil Corp are now typically into the millions," Maarten van Dantzig, Fox-IT security researcher, told ZDNet today. "We've seen demands of more than $10 million," he added. [...] "Typically, they hit file servers, database services, virtual machines, and cloud environments," researchers said.

https://www.zdnet.com/article/new-wastedlocker-ransomware-demands-payments-of-millions-of-usd/

Fxmsp hackers made $1.5M selling access to corporate networks

Fxmsp became widely known outside hacker forums about a year ago when cybersecurity boutique Advanced Intelligence (AdvIntel) published a series of reports on the actor’s attempts to close a $300,000 deal for selling access to networks belonging to Symantec, Trend Micro, and McAfee. [...] According to Yelisey Boguslavskiy, AdvIntel director of security research, Fxmsp was the hacking part of a crew (GPTitan) consisting of specialists "geared to secretly work in financial environments" to steal from high-profile networks data relevant to customers.

https://www.bleepingcomputer.com/news/security/fxmsp-hackers-made-15m-selling-access-to-corporate-networks/

Bungled Lancet study casts shadow over health data industry

The ensuing scandal threw a damper on the idea of medical research being based entirely on big sets of health data, at a time when the market for health data is booming and big industrial players are pushing for its use in medical research. Google this week formally notified the European Commission of its plans to buy wearable health tracking devices company Fitbit — and its troves of sensitive health data — in a deal that has alarmed privacy campaigners, while Palantir, a U.S. data mining company, recently gained access to U.K. health data.

https://www.politico.com/news/2020/06/24/lancet-study-hydroxychloroquine-health-data-industry-337663

3 Key Ways to Bolster Healthcare Cybersecurity with MFA, Training

For the healthcare sector, already burdened with the Coronavirus response, the

expanded threat landscape could lead to some serious issues down the line. Fortunately, the majority of these advisories contain key elements that could allow enterprises to effectively close some of these critical gaps.

- MULTI-FACTOR AUTHENTICATION
- USER EDUCATION, TRAINING
- ASSET INVENTORY AND PATCH MANAGEMENT

https://healthitsecurity.com/news/3-key-ways-to-bolster-healthcare-cybersecurity-with-mfa-training

CISA's Ware Runs Down COVID-19 Cyber Threats to Health Sectors

Despite the massive turn to telework at government agencies and in the private sector during the pandemic – and the accompanying assault of cyber attacks from actors looking to take advantage of the situation – Ware said that CISA has continued on pace with other missions, including effort to secure the national elections in November. He said the "risk picture" for CISA has shown up strongly in four categories: phishing exploit increases; ransomware attacks on healthcare systems; espionage against pharmaceutical companies and laboratories; and risks involved with shift to telework.

https://www.meritalk.com/articles/cisas-ware-runs-down-covid-19-cyber-threats-to-health-sectors/

Indiabulls Group hit by CLOP Ransomware, gets 24h leak deadline

"The Indiabulls Group is a diversified financial services group with interests in housing finance, consumer finance and personal wealth. The Group also has a presence in Real Estate, Pharmaceuticals, Lighting and Infrastructure & Construction Equipment Leasing[.]" [...] Cyberintelligence firm Bad Packets told BleepingComputer, though, that Indiabulls has an Citrix Netscaler ADC VPN gateway exposed, which is vulnerable to the CVE-2019-19781 vulnerability.

https://www.bleepingcomputer.com/news/security/indiabulls-group-hit-by-clop-ransomware-gets-24h-leak-deadline/

FBI, DoJ Officials Warn of Common COVID-19 Cyber Threat Vectors

Tonya Ugoretz, deputy assistant director of the FBI's Cyber Division, reported that the agency's Internet Crime Complaint Center has seen as many complaints as this point in 2020 as they did in all of 2019. Of those complaints, she said at the June 24 Fal.Con for the Public Sector CrowdStrike Cybersecurity Conference, at least 20,000 have been about COVID-19 related schemes.

https://www.meritalk.com/articles/fbi-doj-officials-warn-of-common-covid-19-cyber-threat-vectors/

Banks can ill afford to get complacent about coronavirus

[Cyber] resiliency in a business continuity model is going to be crucial to ensuring a safe and secure financial system. Cyber resiliency is broader than the traditional business continuity focus on data backup and recovery. It's about data integrity and the ability to trust the data to know with confidence that backed-up data has not been corrupted or altered by a cyberattack. Resilience is the ability to operate, even in a degraded state, and recover from deliberate attacks.

https://www.americanbanker.com/opinion/banks-can-ill-afford-to-get-complacent-about-coronavirus

There's No Vaccine For Data Leaks: Why One Cyber Attack Leads To Another

Businesses have become far too accustomed to massive security breaches, disregarding them like the common cold. Often, the remedy appears to be free credit monitoring for the affected. But the real threat is lost in that perception of safety and a healthy bounce-back. Many significant risks are escalated after a breach leveraging the data that is lost in these incidents — stolen personal details enable ransomware or "man-in-the-middle" breaches to be more targeted and effective.

https://www.forbes.com/sites/emilsayegh/2020/06/24/theres-no-vaccine-for-data-leaks-why-one-cyber-attack-leads-to-another/#58d58a757300

Senate wants more clarity on cyber ops

In its version of the annual defense policy bill — which passed the committee last week, though full text of the language was only made public this week — the committee takes aim at U.S. Cyber Command's so-called hunt forward operations. Hunt forward operations involve teams from Cyber Command physically deploying to other nations to assist them with cyber defense. These operations provide American cyber teams insight into tactics that could be turned against U.S. networks or used to disrupt the elections process, officials have maintained.

https://www.fifthdomain.com/congress/2020/06/24/senate-wants-more-clarity-on-cyber-ops/

Cyber attack on Israeli water-treatment plant is one indication of a rising tide of cyber security issues

The water facility attack was to release large amounts of poisonous chlorine into Israel's water delivery infrastructure, potentially poisoning tens of thousands of Israelis. It may indicate a growing threat of cyber attack throughout the world. FireEye, a publicly traded cyber security company in Milpitas, California, determined that the malware developed for this kind of attack came out of Russia and specifically from the Central Scientific Research Institute of Chemistry and Mechanics, a Russian government-owned technical research institution in Moscow.

https://www.militaryaerospace.com/trusted-computing/article/14178333/cyber-security-growing-threat-international-actors

China is Retooling, and Russia Seeks Harm to Critical Infrastructure

China and Russia continue to pose the greatest espionage and cyber attack threats to the United States, but the intelligence leader anticipates that other adversaries and strategic competitors will also build and integrate cyber espionage, cyber attacks and influence operations into how they conduct business. "Our strategic competitors will increasingly use cyber space capabilities including cyber espionage, cyber attack and continued influence operations to seek political, economic and military advantage over the United States, our allies and our partners," he said. "This is not an 'if,' it is a yes. They are doing it and they will continue."

https://www.afcea.org/content/china-retooling-and-russia-seeks-harm-critical-infrastructure

Police arrested wrong man based on facial recognition fail, ACLU says

The American Civil Liberties Union filed the complaint (PDF) Wednesday on behalf of Robert Williams, a Michigan man who was arrested in January based on a false positive generated by facial recognition software. "At every step, DPD's conduct has been improper," the complaint alleges. "It unthinkingly relied on flawed and racist facial recognition technology without taking reasonable measures to verify the information being provided" as part of a "shoddy and incomplete investigation."

https://arstechnica.com/tech-policy/2020/06/police-arrested-wrong-man-based-on-facial-recognition-fail-aclu-says/

Twitter bans DDoSecrets account over 'BlueLeaks' police data dump

On Friday, last week, the group published 296 GB of data they claimed to have received from the Anonymous hacker collective. The data dump, dubbed BlueLeaks, contained millions of documents that were stolen from a Texas company named Netsential that provided web hosting services for various US law enforcement entities. Subsequent analysis revealed that the BlueLeaks data dump contained files from more than 200 US police departments, fusion centers, and other law enforcement training and support portals.

https://www.zdnet.com/article/twitter-bans-ddosecrets-account-over-blueleaks-police-data-dump/

Self-Propagating Lucifer Malware Targets Windows Systems

The never-before-seen malware initially tries to infect PCs by bombarding them with exploits in hopes of taking advantage of an “exhaustive” list of unpatched vulnerabilities. While patches for all the critical and high-severity bugs exist, the various companies impacted by the malware had not applied the fixes. [...] The vulnerabilities targeted by Lucifer include Rejetto HTTP File Server (CVE-2014-6287), Oracle Weblogic (CVE-2017-10271), ThinkPHP RCE (CVE-2018-20062), Apache Struts (CVE-2017-9791), Laravel framework CVE-2019-9081), and

Microsoft Windows (CVE-2017-0144, CVE-2017-0145, and CVE-2017-8464).

https://threatpost.com/self-propagating-lucifer-malware-targets-windows-systems/156883/

Republicans Who Don't Understand Encryption Introduce Bill to Break It

While the senators do name a few instances in which encryption made it harder for the cops to investigate shootings and organized crime, they also chose the well-trodden path of waving their arms and scream about terrorism and protecting children, while blaming tech companies for not doing enough.

https://www.vice.com/en_us/article/y3z3z7/republican-encryption-bill-privacy-signal

You are receiving this email because you are subscribed to receive the IT Security Daily Blast email from Michael Hamilton, Founder, President, and CISO of CI Security, formerly Critical Informatics.

Archived articles are available at https://ci.security/news/daily-news.

CI Security and the CI Security logo are the trademarks of CI Security, Inc. All other brand names, trademarks, service marks, and copyrights are the property of their respective owners.

© 2020 CI Security. All rights reserved.

CI Security

245 4th St, Suite 405 Bremerton, WA 98337

Cybercrime & Application Security Weekly Briefing

From: ImmuniWeb <no-reply@immuniweb.com>

To: jonathan.springborn@cookcountyil.gov, Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>

Sent: June 26, 2020 8:56:32 AM CDT

Received: June 26, 2020 8:56:47 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

ImmuniWeb® AI for Application Security

June 26, 2020

Weekly Briefing

Your weekly briefing on Application Security, AI and Cybercrime:

International Media Coverage

Newsweek

[Activists Drop 270GB 'BlueLeaks' File of Internal Police Documents Online]

June 24, 2020



[Twitter Suspends Account of Organization Behind Police Leaks]

June 24, 2020



[BlueLeaks files expose data from law enforcement, fusion centers]

June 23, 2020



[269GB of data stolen from US police departments published after 'BlueLeaks' hack]

June 23, 2020



[Huge Data Dump of Police Files Dubbed “Blue Leaks” Leaked Online]

June 22, 2020



[North Korea reportedly plans massive cyberattack this weekend to steal your stimulus check]

June 20, 2020



[Report: Lazarus Group has large-scale Covid-19 phishing campaign in the works]

June 19, 2020

Top Rated Articles



Application Penetration Testing

Modern-day application penetration testing (or pentesting) spans from traditional web and mobile app penetration testing to emerging IoT and blockchain penetration testing.



Automated Penetration Testing

Automated penetration testing services and SaaS solutions incrementally substitute traditional human-driven penetration testing, providing greater scalability, efficiency and efficiency and DevSecOps integrations if implemented and conducted correct



[Attack Surface Management]

Attack Surface Management (ASM) is composed of continuous discovery, inventory, classification, prioritization and security monitoring of external digital assets that contain, transmit or process your corporate data.



[Dark Web Monitoring Surface, Deep and Dark Web Explained]

Dark Web monitoring enables organizations to stay ahead of cybercriminals with proactive intelligence on data breaches impacting their internal systems and trusted third-parties, to timely respond to phishing, fraud, Business Email Compromise (BEC) attacks and Intellectual Property infringements.

Application Security Buzz

> #Nvidia squashes display driver code execution, information leak bugs: zdnet.com/article/nvidia… #vulnerabilities #cybersecurity

> #Hackers hide #Magecart script in favicon image's EXIF data to steal credit card

details: computing.co.uk/news/4017010/h… #WebSecurity

#Phishing and #cryptocurrency scams squashed as one million emails are reported to new anti-scam hotline:… twitter.com/i/web/status/1…

Critical Bugs and #Backdoor Found in GeoVision's Fingerprint and Card Scanners: thehackernews.com/2020/06/geovis… #cybersecurity

#GDPR year two report - EU gives itself a pass with high praise: scmagazineuk.com/gdpr-year-two-… #cybersecurity #privacy

Duration of application #DDoS attacks increasing, some go on for days: helpnetsecurity.com/2020/06/25/app… #cyberattacks #WebSecurity

#LG Electronics allegedly hit by Maze #ransomware attack: bleepingcomputer.com/news/security/… #malware #cyberattack

Exposed Frost & Sullivan databases for sale on #hacking forum: bleepingcomputer.com/news/security/… #databreach #privacy

Fake Canadian #COVID19 tracing app with #ransomware discovered: itworldcanada.com/article/fake-c… #MobileSecurity #malware

RT @Newsweek: Activists drop 270GB "BlueLeaks" file of internal police documents online newsweek.com/activists-drop…

Over Two-Thirds of Q1 #Malware Hidden by #HTTPS: infosecurity-magazine.com/news/over-twot… #encryption

RT @SecurityWeek: Twitter Suspends Account of Organization Behind #BlueLeaks Police Leaks securityweek.com/twitter-suspen…

Only 31% of Americans concerned with data security, despite 400% rise in #cyberattacks: techrepublic.com/article/only-3… #cybersecurity

RT @SCMagazine: Activist group DDoSecrets published data that it says was nicked from more than 200 law enforcement agencies and fusion cen…

#Twitter discloses billing info leak after 'data security incident': bleepingcomputer.com/news/security/… #WebSecurity #dataleak

#Hackers Using #Google Analytics to Bypass #WebSecurity and Steal Credit Cards: thehackernews.com/2020/06/google…

Flash-based #MacOS #malware hides in plain sight:

computerweekly.com/news/252485028… #cybersecurity ”

“ 80,000 printers are exposing their IPP port online: zdnet.com/article/80000-… #IoT #cybersecurity ”

“ #Ryuk #ransomware deployed two weeks after #Trickbot infection: bleepingcomputer.com/news/security/… #malware #trojan ”

“ RT @SiliconANGLE: 269GB of data stolen from US police departments published following ‘BlueLeaks’ hack ift.tt/3fMTTu5 ”

“ Huge Data Dump of Police Files Dubbed “#BlueLeaks” Leaked Online: cbronline.com/news/blue-leak… #dataleak #privacy ”

“ £16 million lost to #eCommerce fraud during lockdown: scmagazineuk.com/16-million-los… #COVID19 #cybersecurity ”

“ Stalker Online Breach: 1.3 Million User Records Stolen: infosecurity-magazine.com/news/stalker-o… #privacy #databreach ”

“ Hundreds of US Police Departments Had Their Sensitive Data Leaked: technadu.com/hundreds-of-us… #dataleak #privacy ”

“ Australians reported 25,000 #phishing scams last year: zdnet.com/article/austra… ”

“ RT @tomsguide: North Korea reportedly plans massive cyberattack this weekend to steal your stimulus-check cash tomsguide.com/news/north-kor… http… ”

“ RT @SCMagazine: Report: Lazarus Group has large-scale Covid-19 phishing campaign in the works. #phishing #NorthKorea #LazarusGroup #HiddenC… ”

“ #Mac #malware spreads through malicious results in #Google searches: scmagazineuk.com/mac-malware-sp… ”

“ #Google removes 106 malicious #Chrome extensions that were spying on users: techspot.com/news/85700-goo… #malware #WebSecurity ”

“ #Australia hit with repeated nation-state #cyberattacks: computerweekly.com/news/252484912… #cybercrime ”

“ #Drupal fixes three #vulnerabilities, including one RCE: helpnetsecurity.com/2020/06/19/cve… #exploit #WebSecurity ”

More at twitter.com/immuniweb

ImmuniWeb® Community



Mobile App Security Test

660,742

apps tested



Domain Security Test

916,861,938

domains analyzed



SSL Security Test

59,931,131

servers tested



Website Security Test

48,725,204

servers tested

To unsubscribe from newsletter click here.

© 2020 ImmuniWeb | Privacy Policy

<!

The CyberWire 6.26.20: Exchange bug goes unpatched and exploited. GoldenSpy does your taxes (and spies on you). Magecart evolution. Threat made good.

From: The CyberWire <editor@thecyberwire.com>

To: Keith.Morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: June 26, 2020 10:27:37 AM CDT

Received: June 26, 2020 10:27:54 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

More signal, less noise.

SPONSORED BY RECORDED FUTURE:

Get real-time security intelligence at no cost.

We recently launched Recorded Future Express — a free browser extension for security teams. Use Express over any web-based SIEM, vulnerability management solution, security blog, and more to put real-time security intelligence at your fingertips. Instantly prioritize alerts, incidents, and vulnerabilities based on real-time risk scores from the world's largest commercial collection platform. Sign up now.

Daily briefing.

June 26, 2020.

SUMMARY

By the CyberWire staff

Microsoft continues to urge users of its Exchange email servers to patch and bring them up to date. A known, and it's worth emphasizing patched, vulnerability (CVE-2020-0688) has been under active exploitation by nation-state intelligence services since April. As ZDNet asks, why would any intelligence service worthy of its trenchcoats (we paraphrase and mix many metaphors) burn a zero-day when they could just waltz in through a known hole?

Trustwave says it's found a new malware family, "GoldenSpy," embedded in tax software companies doing business in China have been required by their Chinese bank to install. It does the taxes; it also opens a system-level backdoor.

A Malwarebytes report describes how Magecart operators have improved their game. The paycard skimming malware is now being hidden in EXIF metadata of image files. There are several criminal gangs known to use Magecart. This particular upgrade appears to be the work of Magecart Group 9.

The extortionists who compromised Indiabulls have made good on their threat to begin releasing data if the company didn't pay the ransom. The Hindustan Times reports that the first tranche of company information has been leaked.

Where do vulnerabilities come from? Mostly, according to Snyk's study of open-source software security, from indirect dependencies.

Twitter may have banned DDoSecrets after the BlueLeaks information dump, but DDoSecrets rejects what they call the social platform's unexpectedly "Nixonian" move, and the group tells WIRED they'll be looking for other venues in which to post whatever they come up with in the future.

[250]

SPONSORED BY GDIT:

Secure your mission with the GDIT Cyber Stack, our ecosystem of cyber capabilities.

Notes.

Today's issue includes events affecting Australia, Canada, China, India, Iran, Russia, the United Kingdom, the United States, and Venezuela.

Feedback Friday: Cyber Threat Intelligence Operations

By Rick Howard, CSO, Chief Analyst, and Senior Fellow, The CyberWire

What kind of cyber threat intelligence program do you have? Go to the survey, here, and choose all that apply.

1. What's a cyber threat intelligence program?

2. Somebody in the SOC reads security blogs and listens to the CyberWire every day.
3. I read security blogs and listen to the CyberWire every day.
4. We have a dedicated team of intelligence analysts who read security blogs and listen to the CyberWire every day.
5. We have a dedicated team of intelligence analysts who follow the standard intelligence lifecycle intelligence process.

SPONSORED BY MCAFEE:

Transition your enterprise to a secured, remote work environment with McAfee

Most companies aren't prepared to secure data and assets for a surge of remote employees. Whether your VPN is over capacity, new cloud services are coming on-board, or new devices need protection, we have you covered during this critical time. McAfee is offering 3-month subscriptions for Endpoint Protection, Unified Cloud Edge, and CASB to help you scale security to your remote employees. Learn more about these offers at mcafee.com/workfromhome.

ON THE PODCAST

In today's CyberWire Daily Podcast, out later this afternoon, we speak with Camille Stewart from Google and Lauren Zabierek from Harvard's Belford Center on the #Sharethemicincyber event. Later, we talk with Richard Clarke and Robert Knake, authors of The Fifth Domain.

SPONSORED EVENTS

FutureCon Virtual Eastern Conference (Online, June 30, 2020) This virtual event features thought-provoking presentations by Industry Security Leaders, esteemed Keynote Speakers, and a Panel Session discussion with experienced professionals and a talented team who are at the forefront of cutting edge strategies for Cybersecurity defense. 100% off promo code: CYBERWIRE

IoT Integrator Summit: Securing Edge Computing (Online, July 14 - 16, 2020) A virtual summit to help IoT Integrators learn more about advances and updates in IoT security and discover new methods for architecting IoT solutions for your organization or your clients.

RSA Conference APJ July 15-17, 2020 - A Virtual Learning Experience (Online, July 15 - 17, 2020) The world's leading cybersecurity event is going virtual 15-17 July. Join your peers and industry experts for three days of insights. Watch over 50 sessions live during Singapore business hours—or stream them later. Register today for free.

SELECTED READING

Cyber Attacks, Threats, and Vulnerabilities

Microsoft: Patch your Exchange servers, they're under attack (ZDNet) What attacker needs to risk burning a zero-day flaw when targets leave critical Exchange bugs unpatched...

The cyber honey trap that caught out Beijing (Australian Financial Review) The inside story of the new front line in China's escalating cyber offensive and its most notorious hacking...

Anonymous Activism Through Cyberspace- 2020 Ventures (Modern Diplomacy) In between the hullabaloo of Corona pandemic, the distinct issues in cyberspace are anticipated to rise...

Find MORE on our website.

Security Patches, Mitigations, and Software Updates

Patch time! NVIDIA fixes kernel driver holes on Windows and Linux (Naked Security) Kernel driver bugs often let crooks take over your entire system from even the weediest foothold.

TikTok to stop snooping on users' clipboards after iPhone update shows app constantly reads copied text (The Telegraph) A security patch from Apple has suddenly exposed just how many smartphone apps are reading users' clipboards...

macOS Big Sur vs Catalina: Will it be worth the upgrade? (Macworld UK) There is change coming both on the surface and underneath, but will that be enough to upgrade to Big...

Cyber Trends

Sponsored content: What treadmills tell us about the state of the office during Covid-19. (The CyberWire) (This article was contributed and sponsored by Extrahop.) Everything from IP phones to printers to treadmills...

Hospitals Scramble to Adapt Security Measures Amid Cyberattacks (Wall Street Journal) Hackers are attempting to gain access to hospital financial networks and medical records on a huge scale,...

NetMotion finds that remote employees are dangerously exposed to risky content (NetMotion Software) NetMotion used anonymized data to see whether remote workers put themselves at risk by clicking on risky...

Find MORE on our website.

Marketplace

The 10 biggest cyber security acquisitions of 2020 (so far) (CRN) A leg up on the competition

HelpSystems Acquires Leading Data Classification Providers to Bolster Security Business (HelpSystems) Canada-based Titus and UK-based Boldon James join to create top platform in data classification software...

Qinetiq disposes of Boldon James (BOLSAMANIA) Science and engineering group Qinetiq agreed to dispose of software company Boldon James on Thursday.

Find MORE on our website.

Products, Services, and Solutions

KnowBe4's New CEO Fraud Prevention Manual Now Available (GlobeNewswire) Manual to help security professionals stay better protected from CEO fraud

Veea Brings Enterprise-Grade Security to SMB/SMEs and IoT with New vTPN Security Edge Service (PR Newswire) Veea Inc., a pioneer in smart edge connectivity and computing, today announced the availability of their...

King & Union and DarkOwl Unite to Provide Fractional Access to Searchable Darknet Data (King & Union) DarkOwl Brings World's Largest Database of Darknet Content to King & Union Avalon Cyber Analysis Platform...

Find MORE on our website.

Technologies, Techniques, and Standards

SOAR Is DevSecOps (RSA Conference) In 2016, I was convinced that DevSecOps was the way forward for the network defenders of the world to...

Core cybersecurity principles for new companies and products (Help Net Security) A new World Economic Forum report outlines core cybersecurity principles and points to how companies...

There is no cybersecurity silver bullet (TechRadar) There's no single cybersecurity solution

Find MORE on our website.

Design and Innovation

Facebook will show users a pop-up warning before they share an outdated story (TechCrunch) Facebook announced Thursday that it would introduce a notification screen warning users if they try to...

Marred by garbage: Striking a balance for security data (Help Net Security) One of the most central questions, is how much data is enough? What is the correct balance? Niagara Network...

Research and Development

Quantum entanglement demonstrated aboard orbiting CubeSat: Advance poised to enable cost-effective space-based global quantum network for secure communications and more (ScienceDaily) In a critical step toward creating a global quantum communications network, researchers have generated...

Legislation, Policy, and Regulation

Iran Trains Venezuelan Military to Control Communications (PanAm Post) Nicolás Maduro's regime made Venezuela the country with the largest presence of cyber troops dedicated...

Bid to keep Huawei out of 5G trials (Telegraph) DoT panel to review participation of Chinese companies

Japan Plans National Champion to Challenge Huawei (Wall Street Journal) Japan's top telecommunications company is taking a $600 million stake in a leading telecoms hardware...

Find MORE on our website.

Litigation, Investigation, and Law Enforcement

Trudeau rejects calls to release Huawei executive (BBC News) The PM is under pressure to release Meng Wanzhou in order to help free two detained Canadians.

The Law of Classified Information: A Primer (Lawfare) How the U.S. government regulates its secrets.

New Charges, Sentencing in Satori IoT Botnet Conspiracy (KrebsOnSecurity) The U.S. Justice Department today criminally charged a Canadian and a Northern Ireland man for allegedly...

Find MORE on our website.

INDUSTRY EVENTS

For a complete running list of events, please visit the Event Tracker on the CyberWire website.

Newly Noted Events

Thraxos' Entrepreneur and CXO Forum (Online, July 1, 2020) Thraxos' Entrepreneur and CXO Forum is hosting a panel of experts for a discussion on hot topics in privacy,...

2020 Intelligence & National Security Summit (Online, September 16 - 18, 2020) The nation's premier intelligence and national security conference is going virtual! Taking place Sept...

Upcoming Events

WSIS Forum 2020 (Online, June 22 - September 10, 2020) The World Summit on the Information Society (WSIS) Forum 2020, celebrates 15 years of providing a multi-stakeholder...

Texas Cyber June'gle Virtual Summit (Online, June 27 - 28, 2020) The Texas Cyber June'gle Virtual Summit is June 27th and June 28th, it runs approximately 30 hours straight,...

FutureCon Virtual Eastern Conference (Online, June 30, 2020) This virtual event features thought-provoking presentations by Industry Security Leaders, esteemed Keynote...

CS4CA World: Global Cyber Security Event (Online, June 30, 2020) CS4CA World will take place virtually as a unique large-scale event to keep the critical asset community...

Thraxos' Entrepreneur and CXO Forum (Online, July 1, 2020) Thraxos' Entrepreneur and CXO Forum is hosting a panel of experts for a discussion on hot topics in privacy,...

SPONSOR & SUPPORT

Grow your brand and reach new customers.

Grow your brand and increase your customer base by educating our audience about your products, services, and events by advertising on The CyberWire. We've built trust with an influential (and often hard to reach) audience of CISOs, CSOs, and other senior execs in the security space, across a wide array of industry verticals. Learn more.



Copyright © 2020, CyberWire Inc. Views and assertions of the various sources cited, Selected Reading articles, and cartoons are those of the authors and artists, not the CyberWire, Inc.

This email was sent to Keith.Morrison@cookcountyil.gov
why did I get this? | unsubscribe | update subscription preferences

The CyberWire · 8110 Maple Lawn Blvd. · Suite 200 · Fulton, Md 20759 · USA

NYPD Weekly Terrorism Brief - Issue #26 of 2020

From: NYPD - Intel Analysis Publications <intelanalysispublications@nynjhidta.org>

Sent: June 26, 2020 1:30:18 PM CDT
Received: June 26, 2020 1:31:06 PM CDT
Attachments: NYPD_Weekly Terrorism Brief_26 June 2020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Colleagues,

The latest issue of the NYPD's ***Weekly Terrorism Brief*** is attached.

As a reminder, we request that you **not** forward this product to others.

If you know someone who should be added to the distribution list, please contact the team at IntelAnalysisPublications@nynjhidta.org.

--
NYPD Intelligence Bureau

Confidentiality Notice: This e-mail communication and any attachments contain confidential and privileged information intended solely for the use of the designated recipients named above. If you are not an intended recipient of this communication, or if you have received this communication in error, any review, disclosure, dissemination, distribution or copying of this communication, its contents as well as any attachments, is prohibited and may subject you to prosecution. If you have received this communication in error, please notify the sender immediately by replying to this message and deleting it from your computer.

NYPD Weekly Terrorism Brief - Issue #26 of 2020

Sent: June 26, 2020 1:30:18 PM CDT
Received: June 26, 2020 1:31:08 PM CDT

Top 5 News & Articles of the Week

From: Police Top Stories <PoliceTopStories@bobitenews.com>
To: edward.lewandowski@cookcountyil.gov, Edward Lewandowski (Sheriff) <Edward.Lewandowski@cookcountyil.gov>

Sent: June 27, 2020 10:01:50 AM CDT
Received: June 27, 2020 10:02:18 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Jun 27, 2020 View online version

TOP NEWS

Florida Officers Lured Into Ambush Attack at Call for Service

Several officers with the Tampa (LF) Police Department were reportedly ambushed early Saturday morning while responding to a call for service.

READ MORE

Three North Carolina Officers Fired Over Hate Speech

Piner reportedly said he is “ready” for the civil war and martial law he believes is coming, saying, “we are just gonna go out and start slaughtering them..."

READ MORE

Minneapolis Takes First Steps Toward Disbanding Police Department

The head of the new department would be somebody with "non-law-enforcement experience in community safety services, including but not limited to public health and/or restorative justice approaches."

READ MORE

NYPD Officers May be Planning July 4 Strike, NY Post Reports

The paper says a pair of flyers making the rounds among NYPD officers are encouraging them to call out sick July 4. “NYPD cops will strike on July 4th to let the city have their independence without cops,” the message, which is being passed among cops via text, according to Post sources.

READ MORE

New Jersey Trooper Thrown from Patrol Vehicle in Horrific Crash

A trooper with the New Jersey State Police trooper

was thrown 30 feet from his patrol vehicle in a vehicle collision with a dump truck Monday on the New Jersey Turnpike.

READ MORE

Rasmussen Poll: Majority of Americans Want to Keep Police

A recent poll conducted by Rasmussen indicates that Americans value the role of the police and worry that increasing criticism of cops will make their communities less safe.

READ MORE

Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

READ MORE

Senate Democrats Torpedo GOP's Police Reform Bill

On one major point of dissension between the parties, the Republican bill leaves intact the “qualified immunity” standard that Democrats want to erode, to make it easier for law enforcement officials to be

sued for misconduct.

READ MORE

Hackers Steals Massive Trove of Police Files, Post Them Online

DDoSecrets said the BlueLeaks archive indexes “ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources,” and that “among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more.”

READ MORE

Mock Lynching of Mannequin in Police Uniform Found in Florida

A mock lynching of a mannequin wearing a police uniform was found hanging over an interstate highway in Florida over the weekend.

READ MORE

FREE WHITEPAPERS

- SPECIAL REPORT: Drug Enforcement, Protection & Testing
- Police and the Coronavirus Pandemic
- SPECIAL REPORT: Fleet Management & Upfitting
- Special Report: Preventing & Preparing for Workplace Attacks
- Best Practices for Setting Up and Implementing a First Responder Network
- Special Report: Software & Mobile Apps
- Special Report: Ballistic Protection
- The Top 5 Emerging Technologies Police Agencies Can't Do Without
- How Technology Mitigates Threats at Large-Scale Events
- Special Report: Critical Incident Response
- Special Report: Upfitting & Fleet Management

POLICE MAGAZINE

You are currently subscribed as edward.lewandowski@cookcountyil.gov. Manage your email preferences.

Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Top 5 News & Articles of the Week

To:	Edward Lewandowski (Sheriff)
Sent:	June 27, 2020 10:01:50 AM CDT
Received:	June 27, 2020 10:02:19 AM CDT

Top 5 News & Articles of the Week

From: Police Top Stories <PoliceTopStories@bobitenews.com>
To: larry.schurig@cookcountyil.gov, Larry Schurig (Sheriff) <Larry.Schurig@cookcountyil.gov>
Sent: June 27, 2020 10:03:01 AM CDT
Received: June 27, 2020 10:04:32 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Jun 27, 2020 View online version

TOP NEWS

Florida Officers Lured Into Ambush Attack at Call for Service

Several officers with the Tampa (LF) Police Department were reportedly ambushed early Saturday morning while responding to a call for service.

READ MORE

Three North Carolina Officers Fired Over Hate Speech

Piner reportedly said he is “ready” for the civil war and martial law he believes is coming, saying, “we are just gonna go out and start slaughtering them..."

READ MORE

Minneapolis Takes First Steps Toward Disbanding Police Department

The head of the new department would be somebody with "non-law-enforcement experience in community safety services, including but not limited to public health and/or restorative justice approaches."

READ MORE

NYPD Officers May be Planning July 4 Strike, NY Post Reports

The paper says a pair of flyers making the rounds among NYPD officers are encouraging them to call out sick July 4. “NYPD cops will strike on July 4th to let the city have their independence without cops,” the message, which is being passed among cops via text, according to Post sources.

READ MORE

New Jersey Trooper Thrown from Patrol Vehicle in Horrific Crash

A trooper with the New Jersey State Police trooper

was thrown 30 feet from his patrol vehicle in a vehicle collision with a dump truck Monday on the New Jersey Turnpike.

READ MORE

Rasmussen Poll: Majority of Americans Want to Keep Police

A recent poll conducted by Rasmussen indicates that Americans value the role of the police and worry that increasing criticism of cops will make their communities less safe.

READ MORE

Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

READ MORE

Senate Democrats Torpedo GOP's Police Reform Bill

On one major point of dissension between the parties, the Republican bill leaves intact the “qualified immunity” standard that Democrats want to erode, to make it easier for law enforcement officials to be

sued for misconduct.

READ MORE

Hackers Steals Massive Trove of Police Files, Post Them Online

DDoSecrets said the BlueLeaks archive indexes “ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources,” and that “among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more.”

READ MORE

Mock Lynching of Mannequin in Police Uniform Found in Florida

A mock lynching of a mannequin wearing a police uniform was found hanging over an interstate highway in Florida over the weekend.

READ MORE

FREE WHITEPAPERS

- SPECIAL REPORT: Drug Enforcement, Protection & Testing
- Police and the Coronavirus Pandemic
- SPECIAL REPORT: Fleet Management & Upfitting
- Special Report: Preventing & Preparing for Workplace Attacks
- Best Practices for Setting Up and Implementing a First Responder Network
- Special Report: Software & Mobile Apps
- Special Report: Ballistic Protection
- The Top 5 Emerging Technologies Police Agencies Can't Do Without
- How Technology Mitigates Threats at Large-Scale Events
- Special Report: Critical Incident Response
- Special Report: Upfitting & Fleet Management

POLICE MAGAZINE

You are currently subscribed as larry.schurig@cookcountyil.gov. Manage your email preferences.

Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Top 5 News & Articles of the Week

From: Police Top Stories <PoliceTopStories@bobitenews.com>
To: brian.white@cookcountyil.gov, Brian White (Sheriff) <Brian.White@cookcountyil.gov>
Sent: June 27, 2020 10:05:26 AM CDT
Received: June 27, 2020 10:05:37 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Jun 27, 2020 View online version

TOP NEWS

Florida Officers Lured Into Ambush Attack at Call for Service

Several officers with the Tampa (LF) Police Department were reportedly ambushed early Saturday morning while responding to a call for service.

READ MORE

Three North Carolina Officers Fired Over Hate Speech

Piner reportedly said he is “ready” for the civil war and martial law he believes is coming, saying, “we are just gonna go out and start slaughtering them..."

READ MORE

Minneapolis Takes First Steps Toward Disbanding Police Department

The head of the new department would be somebody with "non-law-enforcement experience in community safety services, including but not limited to public health and/or restorative justice approaches."

READ MORE

NYPD Officers May be Planning July 4 Strike, NY Post Reports

The paper says a pair of flyers making the rounds among NYPD officers are encouraging them to call out sick July 4. “NYPD cops will strike on July 4th to let the city have their independence without cops,” the message, which is being passed among cops via text, according to Post sources.

READ MORE

New Jersey Trooper Thrown from Patrol Vehicle in Horrific Crash

A trooper with the New Jersey State Police trooper

was thrown 30 feet from his patrol vehicle in a vehicle collision with a dump truck Monday on the New Jersey Turnpike.

READ MORE

Rasmussen Poll: Majority of Americans Want to Keep Police

A recent poll conducted by Rasmussen indicates that Americans value the role of the police and worry that increasing criticism of cops will make their communities less safe.

READ MORE

Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

READ MORE

Senate Democrats Torpedo GOP's Police Reform Bill

On one major point of dissension between the parties, the Republican bill leaves intact the “qualified immunity” standard that Democrats want to erode, to make it easier for law enforcement officials to be

sued for misconduct.

READ MORE

Hackers Steals Massive Trove of Police Files, Post Them Online

DDoSecrets said the BlueLeaks archive indexes “ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources,” and that “among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more.”

READ MORE

Mock Lynching of Mannequin in Police Uniform Found in Florida

A mock lynching of a mannequin wearing a police uniform was found hanging over an interstate highway in Florida over the weekend.

READ MORE

FREE WHITEPAPERS

- SPECIAL REPORT: Drug Enforcement, Protection & Testing
- Police and the Coronavirus Pandemic
- SPECIAL REPORT: Fleet Management & Upfitting
- Special Report: Preventing & Preparing for Workplace Attacks
- Best Practices for Setting Up and Implementing a First Responder Network
- Special Report: Software & Mobile Apps
- Special Report: Ballistic Protection
- The Top 5 Emerging Technologies Police Agencies Can't Do Without
- How Technology Mitigates Threats at Large-Scale Events
- Special Report: Critical Incident Response
- Special Report: Upfitting & Fleet Management

POLICE MAGAZINE

You are currently subscribed as brian.white@cookcountyil.gov. Manage your email preferences.

Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Google Alert - "Chicago" "Protest"

From: Google Alerts <googlealerts-noreply@google.com>
To: SThompsonCCSO@gmail.com
Sent: June 27, 2020 2:10:58 PM CDT
Received: June 27, 2020 2:11:04 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

"Chicago" "Protest"

Daily update · June 27, 2020

NEWS

Young novice **protest** leaders help drive US wave of dissent
Chicago Sun-Times

Eva Maria Lewis, 21, is an activist in **Chicago** who has been speaking out since she was 16. By Associated Press Jun 27, 2020, 10:23am CDT. Lindsay ...

Flag as irrelevant

Retired Black Cops Kneel In **Protest** Against White Union Leadership
WBEZ

About two-dozen Black former cops and community allies **protest** outside the Fraternal Order of Police Lodge 7 hall on **Chicago's** West Side Friday.

Flag as irrelevant

John Carlos, US athletes take stand to end Olympic **protest** rule
Chicago Sun-Times

Carlos and Tommie Smith raised their fists on the medals stand at the 1968 Mexico City Olympics to **protest** racial inequality in the United States.

Flag as irrelevant

Indian-American community **protest** outside Chinese Consulate in **Chicago**
ANI News

Indian-American community **protest** outside Chinese Consulate in **Chicago**. ANI | Updated: Jun 27, 2020 01:56 IST. **Chicago** ...

Flag as irrelevant

USA: Protesters stage 'anti-China' **protest** outside Chinese Consulate in **Chicago**

Economic Times

USA: Protesters stage 'anti-China' **protest** outside Chinese Consulate in **Chicago**. ANI | 27 Jun 2020, 06:38 AM IST. Post a Comment. Copy URL.

Flag as irrelevant

Protests Planned Around **Chicago** Area in Support of Black Lives Matter Movement

NBC Chicago

At 1 p.m. in suburban Midlothian, a **protest** will take place in the parking lot of the Walgreens location at 147th and Cicero. According to event organizers, ...

Flag as irrelevant

Family demands answers in death of Jamal Williams, fatally shot at Community Hospital in Munster

Chicago Tribune

“He met up with some friends there and made new friends, and he was just blown away by the music,” Imani Williams, 26 and of **Chicago**, said.

Flag as irrelevant

Afternoon Edition: June 26, 2020

Chicago Sun-Times

In **Chicago**, hundreds of prisoners, including some of the nation's most ... When the initially peaceful **protest** turned violent, Hollingsworth realized he ...

Flag as irrelevant

Law Enforcement Scoured Protester Communications and Exaggerated Threats to Minneapolis ...

The Intercept

The agencies also tracked Facebook RSVPs to peaceful **protest** events, ... they also suggest a tendency to categorize standard **protest** behavior as a ... and “busloads of people coming from **Chicago**” headed to the **protest** area.

Flag as irrelevant

Aurora man charged with throwing explosive device that injured police officers during Naperville ...

WLS-TV

Naperville police said during a **protest** on June 1, someone threw multiple explosive devices, causing minor injuries to several officers. Christian Rea, 19 ...

Flag as irrelevant

See more results | Edit this alert

You have received this email because you have subscribed to **Google Alerts**.

Unsubscribe | View all your alerts

Receive this alert as RSS feed

Send Feedback

Google Alert - "Chicago" "Protest"

To:	SThompsonCCSO@gmail.com
Sent:	June 27, 2020 2:10:58 PM CDT
Received:	June 27, 2020 2:11:05 PM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Scott.Lefko@cookcountyil.gov, Scott Lefko (Sheriff) <Scott.Lefko@cookcountyil.gov>

Sent: June 28, 2020 7:44:52 AM CDT
Received: June 28, 2020 7:45:43 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: phillip.mackey@cookcountyil.gov, Phillip Mackey (Sheriff) <Phillip.Mackey@cookcountyil.gov>

Sent: June 28, 2020 7:44:52 AM CDT
Received: June 28, 2020 7:45:09 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: ricky.soto@cookcountyil.gov, Ricky Soto (Sheriff) <Ricky.Soto@cookcountyil.gov>

Sent: June 28, 2020 7:44:52 AM CDT
Received: June 28, 2020 7:45:06 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: joseph.scofield@cookcountyil.gov, Joseph Scofield (Sheriff) <Joseph.Scofield@cookcountyil.gov>

Sent: June 28, 2020 7:44:52 AM CDT
Received: June 28, 2020 7:45:26 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: martin.bennett@cookcountyil.gov, Martin Bennett (Sheriff) <Martin.Bennett@cookcountyil.gov>

Sent: June 28, 2020 7:44:52 AM CDT
Received: June 28, 2020 7:45:13 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Scott Lefko (Sheriff)
Sent: June 28, 2020 7:44:52 AM CDT
Received: June 28, 2020 7:45:44 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: timothy.odonnell@cookcountyil.gov, Timothy O'Donnell (Sheriff) <Timothy.Odonnell@cookcountyil.gov>

Sent: June 28, 2020 7:44:57 AM CDT
Received: June 28, 2020 7:46:18 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: james.minor@cookcountyil.gov, James Minor (Sheriff) <James.Minor@cookcountyil.gov>

Sent: June 28, 2020 7:44:57 AM CDT
Received: June 28, 2020 7:46:35 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: christina.graf@cookcountyil.gov, Christina Graf (Sheriff) <Christina.Graf@cookcountyil.gov>

Sent: June 28, 2020 7:44:57 AM CDT
Received: June 28, 2020 7:46:45 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: henry.hemphill@cookcountyil.gov, Henry Hemphill (Sheriff) <Henry.Hemphill@cookcountyil.gov>

Sent: June 28, 2020 7:44:57 AM CDT
Received: June 28, 2020 7:46:47 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: James Minor (Sheriff)
Sent: June 28, 2020 7:44:57 AM CDT
Received: June 28, 2020 7:46:35 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To: Christina Graf (Sheriff)
Sent: June 28, 2020 7:44:57 AM CDT
Received: June 28, 2020 7:46:45 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: michael.gercone@cookcountyil.gov, Michael Gercone (Sheriff) <Michael.Gercone@cookcountyil.gov>

Sent: June 28, 2020 7:45:23 AM CDT
Received: June 28, 2020 7:45:35 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: sajid.haidari@cookcountyil.gov, Sajid Haidari (Sheriff) <Sajid.Haidari@cookcountyil.gov>

Sent: June 28, 2020 7:45:23 AM CDT
Received: June 28, 2020 7:45:52 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To:	Michael Gercone (Sheriff)
Sent:	June 28, 2020 7:45:23 AM CDT
Received:	June 28, 2020 7:45:35 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To: Sajid Haidari (Sheriff)
Sent: June 28, 2020 7:45:23 AM CDT
Received: June 28, 2020 7:45:53 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: nathan.camer@cookcountyil.gov, Nathan Camer (Sheriff) <Nathan.Camer@cookcountyil.gov>

Sent: June 28, 2020 7:45:29 AM CDT
Received: June 28, 2020 7:46:59 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: eroedel@cookcountygov.com, Erik Roedel (Sheriff) <Erik.Roedel@cookcountyil.gov>

Sent: June 28, 2020 7:45:29 AM CDT
Received: June 28, 2020 7:46:59 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: kendall.evans@cookcountyil.gov, Kendall Evans (Sheriff) <Kendall.Evans@cookcountyil.gov>

Sent: June 28, 2020 7:45:29 AM CDT
Received: June 28, 2020 7:47:18 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: david.cammack@cookcountyil.gov, David Cammack (Sheriff) <David.Cammack@cookcountyil.gov>

Sent: June 28, 2020 7:45:29 AM CDT
Received: June 28, 2020 7:47:13 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: amolina@cookcountygov.com, Adrian Molina (Sheriff) <Adrian.Molina@cookcountyil.gov>

Sent: June 28, 2020 7:45:29 AM CDT
Received: June 28, 2020 7:46:48 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: kyara.lee@cookcountyil.gov, Kyara Lee (Sheriff) <Kyara.Lee@cookcountyil.gov>
Sent: June 28, 2020 7:45:29 AM CDT
Received: June 28, 2020 7:47:14 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Kendall Evans (Sheriff)
Sent: June 28, 2020 7:45:29 AM CDT
Received: June 28, 2020 7:47:19 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To:	Kyara Lee (Sheriff)
Sent:	June 28, 2020 7:45:29 AM CDT
Received:	June 28, 2020 7:47:14 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: rlobacz@cookcountygov.com, Robert Lobacz (Sheriff) <Robert.Lobacz@cookcountyil.gov>

Sent: June 28, 2020 7:45:30 AM CDT
Received: June 28, 2020 7:47:03 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: joseph.bellettiere@cookcountyil.gov, Joseph Bellettiere (Sheriff) <Joseph.Bellettiere@cookcountyil.gov>

Sent: June 28, 2020 7:45:30 AM CDT
Received: June 28, 2020 7:47:03 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: patrick.dwyer@cookcountyil.gov, Patrick Dwyer (Sheriff) <Patrick.Dwyer@cookcountyil.gov>

Sent: June 28, 2020 7:45:30 AM CDT
Received: June 28, 2020 7:47:18 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: tstajura@cookcountygov.com, Theodore Stajura (Sheriff) <Theodore.Stajura@cookcountyil.gov>

Sent: June 28, 2020 7:45:30 AM CDT
Received: June 28, 2020 7:47:10 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: theodore.stajura@cookcountyil.gov, Theodore Stajura (Sheriff) <Theodore.Stajura@cookcountyil.gov>

Sent: June 28, 2020 7:45:33 AM CDT
Received: June 28, 2020 7:47:50 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: tarra.danielsdavis@cookcountyil.gov, Tarra Daniels-Davis (Sheriff) <Tarra.Daniels-Davis@cookcountyil.gov>

Sent: June 28, 2020 7:45:41 AM CDT
Received: June 28, 2020 7:47:33 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: brian.white@cookcountyil.gov, Brian White (Sheriff) <Brian.White@cookcountyil.gov>

Sent: June 28, 2020 7:45:41 AM CDT
Received: June 28, 2020 7:47:47 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: keith.morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: June 28, 2020 7:45:41 AM CDT
Received: June 28, 2020 7:47:39 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: terrence.doran@cookcountyil.gov, Terrence Doran (Sheriff) <Terrence.Doran@cookcountyil.gov>

Sent: June 28, 2020 7:45:41 AM CDT
Received: June 28, 2020 7:47:28 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: ycollins@cookcountygov.com, Yolanda Collins-Watson (Sheriff) <Yolanda.Collins-Watson@cookcountyil.gov>

Sent: June 28, 2020 7:45:42 AM CDT
Received: June 28, 2020 7:47:51 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: andre.blue@cookcountyil.gov, Andre Blue (Sheriff) <Andre.Blue@cookcountyil.gov>

Sent: June 28, 2020 7:45:42 AM CDT
Received: June 28, 2020 7:47:59 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Yolanda Collins-Watson (Sheriff)
Sent: June 28, 2020 7:45:42 AM CDT
Received: June 28, 2020 7:47:52 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: brian.staudt@cookcountyil.gov, Brian Staudt (Sheriff) <Brian.Staudt@cookcountyil.gov>

Sent: June 28, 2020 7:45:45 AM CDT
Received: June 28, 2020 7:50:09 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: mweres@cookcountygov.com, Myron Weres (Sheriff) <Myron.Weres@cookcountyil.gov>

Sent: June 28, 2020 7:45:45 AM CDT
Received: June 28, 2020 7:48:40 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: myron.weres@cookcountyil.gov, Myron Weres (Sheriff) <Myron.Weres@cookcountyil.gov>

Sent: June 28, 2020 7:45:45 AM CDT
Received: June 28, 2020 7:48:27 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: fulvio.compagnone@cookcountyil.gov, Fulvio Compagnone (Sheriff) <Fulvio.Compagnone@cookcountyil.gov>

Sent: June 28, 2020 7:45:45 AM CDT
Received: June 28, 2020 7:48:27 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To:	Myron Weres (Sheriff)
Sent:	June 28, 2020 7:45:45 AM CDT
Received:	June 28, 2020 7:48:40 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Phillip.lapuma@cookcountyil.gov, Philip Lapuma (Sheriff) <Philip.Lapuma@cookcountyil.gov>

Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:50:26 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: jennifer.bordoshuk@cookcountyil.gov, Jennifer Bordoshuk (Sheriff) <Jennifer.Bordoshuk@cookcountyil.gov>

Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:50:22 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: philip.koenig@cookcountyil.gov, Philip Koenig (Sheriff) <Philip.Koenig@cookcountyil.gov>

Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:49:11 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Clarance.Hummel@CookCountyIl.Gov, Clarance Hummel (Sheriff) <Clarance.Hummel@cookcountyil.gov>

Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:49:16 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: daniel.redican@cookcountyil.gov, Daniel Redican (Sheriff) <Daniel.Redican@cookcountyil.gov>

Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:49:18 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: jaunesh.carpenter@cookcountyil.gov, Jaunesh Contreras (Sheriff) <Jaunesh.Contreras@cookcountyil.gov>

Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:49:20 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Joseph.nicholas@cookcountyil.gov, Joseph Nicholas (Sheriff) <Joseph.Nicholas@cookcountyil.gov>

Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:49:19 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: jasmina.janjic@cookcountyil.gov, Jasmina Janjic (Sheriff) <Jasmina.Janjic@cookcountyil.gov>

Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:49:18 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: john.merola@cookcountyil.gov, John Merola (Sheriff) <John.Merola@cookcountyil.gov>

Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:50:35 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Philip Lapuma (Sheriff)
Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:50:27 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To: Jennifer Bordoshuk (Sheriff)
Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:50:23 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To: Philip Koenig (Sheriff)
Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:49:11 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To: Clarance Hummel (Sheriff)
Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:49:17 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To: Jasmina Janjic (Sheriff)
Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:49:18 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To: John Merola (Sheriff)
Sent: June 28, 2020 7:46:08 AM CDT
Received: June 28, 2020 7:50:35 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: walter.klinger@cookcountyil.gov, Walter Klinger (Sheriff) <Walter.Klinger@cookcountyil.gov>

Sent: June 28, 2020 7:46:15 AM CDT
Received: June 28, 2020 7:47:56 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: antonio.imhof@cookcountyil.gov, Antonio Imhof (Sheriff) <Antonio.Imhof@cookcountyil.gov>

Sent: June 28, 2020 7:46:15 AM CDT
Received: June 28, 2020 7:47:22 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: philip.fraticola@cookcountyil.gov, Philip Fraticola (Sheriff) <Philip.Fraticola@cookcountyil.gov>

Sent: June 28, 2020 7:46:15 AM CDT
Received: June 28, 2020 7:47:41 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: stavone.mcherron@cookcountyil.gov, Stavone McHerron (Sheriff) <Stavone.Mcherron@cookcountyil.gov>

Sent: June 28, 2020 7:46:15 AM CDT
Received: June 28, 2020 7:48:06 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: marianne.kelly@cookcountyil.gov, Marianne Kelly (Sheriff) <Marianne.Kelly@cookcountyil.gov>

Sent: June 28, 2020 7:46:15 AM CDT
Received: June 28, 2020 7:47:17 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Gustavo.jimenezjr@cookcountyil.gov, Gustavo Jimenez (Sheriff) <Gustavo.Jimenez@cookcountyil.gov>

Sent: June 28, 2020 7:46:15 AM CDT
Received: June 28, 2020 7:47:39 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Antonio Imhof (Sheriff)
Sent: June 28, 2020 7:46:15 AM CDT
Received: June 28, 2020 7:47:23 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To:	Philip Fraticola (Sheriff)
Sent:	June 28, 2020 7:46:15 AM CDT
Received:	June 28, 2020 7:47:41 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To: Marianne Kelly (Sheriff)
Sent: June 28, 2020 7:46:15 AM CDT
Received: June 28, 2020 7:47:18 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: thomas.goshen@cookcountyil.gov, Thomas Goshen (Sheriff) <Thomas.Goshen@cookcountyil.gov>

Sent: June 28, 2020 7:46:26 AM CDT
Received: June 28, 2020 7:48:25 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: michelle.kaechele@cookcountyil.gov, Michelle Kaechele (Sheriff) <Michelle.Kaechele@cookcountyil.gov>

Sent: June 28, 2020 7:46:26 AM CDT
Received: June 28, 2020 7:48:25 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Rebecca.DeJesus@cookcountyil.gov, Rebecca Dejesus (Sheriff) <Rebecca.Dejesus@cookcountyil.gov>

Sent: June 28, 2020 7:46:26 AM CDT
Received: June 28, 2020 7:48:50 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Albert.Carter@cookcountyil.gov, Albert Carter (Sheriff) <Albert.Carter@cookcountyil.gov>

Sent: June 28, 2020 7:46:26 AM CDT
Received: June 28, 2020 7:48:43 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Richard.obrien2@cookcountyil.gov, Richard O'Brien (Sheriff) <richard.obrien2@cookcountyil.gov>

Sent: June 28, 2020 7:46:26 AM CDT
Received: June 28, 2020 7:48:16 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: aaron.harris@cookcountyil.gov, Aaron Harris (Sheriff) <Aaron.Harris@cookcountyil.gov>

Sent: June 28, 2020 7:46:26 AM CDT
Received: June 28, 2020 7:48:19 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: christopher.harvey@cookcountyil.gov, Christopher Harvey (Sheriff) <Christopher.Harvey@cookcountyil.gov>

Sent: June 28, 2020 7:46:26 AM CDT
Received: June 28, 2020 7:48:58 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Thomas Goshen (Sheriff)
Sent: June 28, 2020 7:46:26 AM CDT
Received: June 28, 2020 7:48:26 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To: Michelle Kaechele (Sheriff)
Sent: June 28, 2020 7:46:26 AM CDT
Received: June 28, 2020 7:48:26 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To: Albert Carter (Sheriff)
Sent: June 28, 2020 7:46:26 AM CDT
Received: June 28, 2020 7:48:43 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To: Aaron Harris (Sheriff)
Sent: June 28, 2020 7:46:26 AM CDT
Received: June 28, 2020 7:48:20 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: michael.rowe@cookcountyil.gov, Michael Rowe (Sheriff) <Michael.Rowe@cookcountyil.gov>

Sent: June 28, 2020 7:46:35 AM CDT
Received: June 28, 2020 7:49:50 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: thomas.staples@cookcountyil.gov, Thomas Staples (Sheriff) <Thomas.Staples@cookcountyil.gov>

Sent: June 28, 2020 7:46:35 AM CDT
Received: June 28, 2020 7:50:55 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Thomas Staples (Sheriff)
Sent: June 28, 2020 7:46:35 AM CDT
Received: June 28, 2020 7:50:56 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: katerina.klopas@cookcountyil.gov, Katerina Klopas (Sheriff) <Katerina.Klopas@cookcountyil.gov>

Sent: June 28, 2020 7:46:44 AM CDT
Received: June 28, 2020 7:47:02 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Randall.Pochie@cookcountyil.gov, Randall Pochie (Sheriff) <Randall.Pochie@cookcountyil.gov>

Sent: June 28, 2020 7:46:44 AM CDT
Received: June 28, 2020 7:47:23 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Katerina Klopas (Sheriff)
Sent: June 28, 2020 7:46:44 AM CDT
Received: June 28, 2020 7:47:02 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To: Randall Pochie (Sheriff)
Sent: June 28, 2020 7:46:44 AM CDT
Received: June 28, 2020 7:47:23 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: agoulos@cookcountygov.com, Anastasios Goulos (Sheriff) <Anastasios.Goulos@cookcountyil.gov>

Sent: June 28, 2020 7:46:57 AM CDT
Received: June 28, 2020 7:47:29 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: debra.clark@cookcountyil.gov, Debra Clark (Sheriff) <Debra.Clark@cookcountyil.gov>

Sent: June 28, 2020 7:46:58 AM CDT
Received: June 28, 2020 7:47:53 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: neal.gaynor@cookcountyil.gov, Neal Gaynor (Sheriff) <Neal.Gaynor@cookcountyil.gov>

Sent: June 28, 2020 7:46:58 AM CDT
Received: June 28, 2020 7:47:43 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: carl.price@cookcountyil.gov, Carl Price (Sheriff) <Carl.Price@cookcountyil.gov>
Sent: June 28, 2020 7:46:58 AM CDT
Received: June 28, 2020 7:47:51 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Debra Clark (Sheriff)
Sent: June 28, 2020 7:46:58 AM CDT
Received: June 28, 2020 7:47:54 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: anthony.sevening@cookcountyil.gov, Anthony Sevening (Sheriff) <Anthony.Sevening@cookcountyil.gov>

Sent: June 28, 2020 7:47:21 AM CDT
Received: June 28, 2020 7:48:13 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Anthony Sevening (Sheriff)
Sent: June 28, 2020 7:47:21 AM CDT
Received: June 28, 2020 7:48:14 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: arthur.jackson@cookcountyil.gov, Arthur Jackson (Sheriff) <Arthur.Jackson@cookcountyil.gov>

Sent: June 28, 2020 7:47:30 AM CDT
Received: June 28, 2020 7:48:18 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Miguel.Mancha@cookcountyil.gov, Miguel Mancha (Sheriff) <Miguel.Mancha@cookcountyil.gov>

Sent: June 28, 2020 7:47:44 AM CDT
Received: June 28, 2020 7:48:51 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: jazmond.watson@cookcountyil.gov, Jazmond Watson (Sheriff) <Jazmond.Watson@cookcountyil.gov>

Sent: June 28, 2020 7:47:44 AM CDT
Received: June 28, 2020 7:48:41 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Miguel Mancha (Sheriff)
Sent: June 28, 2020 7:47:44 AM CDT
Received: June 28, 2020 7:48:52 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: patricia.echols@cookcountyil.gov, Patricia Montgomery-Echols (Sheriff) <Patricia.Montgomery-echols@cookcountyil.gov>

Sent: June 28, 2020 7:47:45 AM CDT
Received: June 28, 2020 7:49:02 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: george.winistorfer@cookcountyil.gov, George Winistorfer (Sheriff) <George.Winistorfer@cookcountyil.gov>

Sent: June 28, 2020 7:47:58 AM CDT
Received: June 28, 2020 7:48:13 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: jclaudio@cookcountygov.com, Juan Claudio (Sheriff) <Juan.Claudio@cookcountyil.gov>

Sent: June 28, 2020 7:47:58 AM CDT
Received: June 28, 2020 7:48:15 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: jrosenau@cookcountygov.com, Joseph Rosenau (Sheriff) <Joseph.Rosenau@cookcountyil.gov>

Sent: June 28, 2020 7:47:58 AM CDT
Received: June 28, 2020 7:48:18 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Joseph.Phillips@cookcountyil.gov, Joseph Phillips (Sheriff) <Joseph.Phillips@cookcountyil.gov>

Sent: June 28, 2020 7:47:58 AM CDT
Received: June 28, 2020 7:48:25 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: juan.claudio@cookcountyil.gov, Juan Claudio (Sheriff) <Juan.Claudio@cookcountyil.gov>

Sent: June 28, 2020 7:47:59 AM CDT
Received: June 28, 2020 7:48:38 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: nicky.nunez@cookcountyil.gov, Nicky Nunez (Sheriff) <Nicky.Nunez@cookcountyil.gov>

Sent: June 28, 2020 7:48:06 AM CDT
Received: June 28, 2020 7:49:27 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Nicky Nunez (Sheriff)
Sent: June 28, 2020 7:48:06 AM CDT
Received: June 28, 2020 7:49:27 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: antoinette.steele@cookcountyil.gov, Antoinette Bradley (Sheriff) <Antoinette.Bradley@cookcountyil.gov>

Sent: June 28, 2020 7:48:12 AM CDT
Received: June 28, 2020 7:48:47 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: ccspdtraining@cookcountygov.com, Sheriff Training (Sheriff) <Sheriff.Training@cookcountyil.gov>

Sent: June 28, 2020 7:48:32 AM CDT
Received: June 28, 2020 7:49:32 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To:	Sheriff Training (Sheriff)
Sent:	June 28, 2020 7:48:32 AM CDT
Received:	June 28, 2020 7:49:32 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: mgoral@cookcountygov.com, Matthew Goral (Sheriff) <Matthew.Goral@cookcountyil.gov>

Sent: June 28, 2020 7:48:43 AM CDT
Received: June 28, 2020 7:49:02 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: rogelio.martinez@cookcountyil.gov, Rogelio Martinez (Sheriff) <Rogelio.Martinez@cookcountyil.gov>

Sent: June 28, 2020 7:48:50 AM CDT
Received: June 28, 2020 7:48:58 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Rogelio Martinez (Sheriff)
Sent: June 28, 2020 7:48:50 AM CDT
Received: June 28, 2020 7:48:59 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Ryan.Huber@cookcountyil.gov, Ryan Huber (Sheriff) <Ryan.Huber@cookcountyil.gov>

Sent: June 28, 2020 7:49:23 AM CDT
Received: June 28, 2020 7:49:34 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To: Ryan Huber (Sheriff)
Sent: June 28, 2020 7:49:23 AM CDT
Received: June 28, 2020 7:49:35 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Marcus.jackson@cookcountyil.gov, Marcus Jackson (Sheriff) <Marcus.Jackson@cookcountyil.gov>

Sent: June 28, 2020 7:49:25 AM CDT
Received: June 28, 2020 7:50:01 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To:	Marcus Jackson (Sheriff)
Sent:	June 28, 2020 7:49:25 AM CDT
Received:	June 28, 2020 7:50:01 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Erica.pepper@cookcountyil.gov, Erica Pepper (Sheriff) <Erica.Pepper@cookcountyil.gov>

Sent: June 28, 2020 7:49:28 AM CDT
Received: June 28, 2020 7:50:56 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: Ron.avelino@cookcountyil.gov, Ron Avelino (Sheriff) <Ron.Avelino@cookcountyil.gov>

Sent: June 28, 2020 7:49:28 AM CDT
Received: June 28, 2020 7:51:17 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

To:	Erica Pepper (Sheriff)
Sent:	June 28, 2020 7:49:28 AM CDT
Received:	June 28, 2020 7:50:57 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

To: Ron Avelino (Sheriff)
Sent: June 28, 2020 7:49:28 AM CDT
Received: June 28, 2020 7:51:17 AM CDT

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: trohl@cookcountygov.com, Todd Rohl (Sheriff) <Todd.Rohl@cookcountyil.gov>
Sent: June 28, 2020 7:49:53 AM CDT
Received: June 28, 2020 7:50:16 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

Cadet death, 'BlueLeaks' hack & other top stories

From: P1 Weekend Rewind <newsletter@policeone.com>
To: mgoldsmith@cookcountygov.com, Michael Goldsmith (Sheriff) <Michael.Goldsmith@cookcountyil.gov>

Sent: June 28, 2020 7:49:53 AM CDT
Received: June 28, 2020 7:50:19 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

June 28, 2020 | View as webpage

FEATURED CONTENT

Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices

Police: Missing girls were never at Milwaukee home set afire

The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured

Academy cadet dies after training exercise

Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation app replaces traditional and expensive communications tools from the past.

Read the article

World Class Performance Has Arrived!

Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan

The legislation creates a $25,000 personal liability ceiling for officers found liable for state constitutional violations

My five sense worth on police reform

By Lt. Dan Marcou

We must address some critical issues of grave importance to the survival of our honorable profession

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

[GovQA] FOIA Request - New Assignment - R009142-062920

From: Cook County Sheriff's Office <cookcountysheriff@govqa.us>
To: Eryn.Hedderman@cookcountyil.gov, Eryn Hedderman (Sheriff) <Eryn.Hedderman@cookcountyil.gov>
Sent: June 29, 2020 3:38:03 AM CDT
Received: June 29, 2020 3:38:08 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

A request has been assigned to you: FOIA Request / R009142-062920

FOIA Request for Records
Assigned Staff: Eryn Hedderman
Status: Received
Create Date: June 29, 2020
Due Date: July 06, 2020
Name of Requester: Emma Best
Requester Affiliation: Press
Record(s) Requested: To Whom It May Concern: Pursuant to the Illinois Freedom of Information Act., I hereby request the following records: 1. Documents mentioning, describing or generated in response to the BlueLeaks release, the preceding hack or subsequent fallout, including but not limited to: * Damage assessments * Emails * Interagency communications (local, state, or federal) * Communications with the press about BlueLeaks * Communications with Twitter or other social media or sharing platforms 2. Documents mentioning or describing Distributed Denial of Secrets (DDoSecrets) You may limit this request to records generated between November 1, 2018 and the present. I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers in outlets such as Gizmodo, MuckRock, Motherboard, Property of the People, Unicorn Riot, and The Outline, among others. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the library Internet Archive and the journalist non-profit MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself. As such, it is not necessary for me to demonstrate the relevance of this particular subject in advance. As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived. The requested documents will be made available to the general public, and this request is not being made for commercial purposes. In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not. Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 5 business days, as the statute requires. Sincerely, Emma Best Upload documents directly: https://https://www.muckrock.comhttps://accounts.muckrock.com/accounts/login/?next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fcook-county-sheriff-719%252Fblueleaks-cook-county-sheriff-96941%252F%253F&url_auth_token=AAAaaJnszUVssmdgx6fh2R-tE3U%3A1jppAE%3ADWZbgy7n864OATjAMxtAsPZltYs

Login to the system and view your request by clicking HERE. Your username and password is the same as your Active Directory login, used to access all CCSO computers. If you have any questions or concerns regarding this email notification, please contact the Legal Department at 312-603-6444.

This is an auto-generated email and has originated from an unmonitored email account. Please DO NOT REPLY to this email as the contents of your response and any attachments may be externally disseminated inadvertently. Click the link above to respond and upload documents for secure internal review.

(U//FOUO) IIB: Criminal Hackers Target US Law Enforcement Data, dated 29 June 2020

From:	CPIC <CPIC@chicagopolice.org>
Sent:	June 29, 2020 10:22:25 AM CDT
Received:	June 29, 2020 10:26:07 AM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

ALCON:

Please see attached product entitled, (U//FOUO) Intelligence in Brief: Criminal Hackers Target US Law Enforcement Data.

(U//FOUO) Intended Audience: Federal, state, and local homeland security officials and authorized critical infrastructure, key resource personnel, and private sector security officials

Chicago Police Department
Crime Prevention and Information Center (CPIC)
Fusion Center
312-745-5669, Fax 312-745-6927

THE CONTENT OF THIS DOCUMENT MAY BE LAW ENFORCEMENT SENSITIVE (LES) &/OR FOR OFFICIAL USE ONLY (FOUO). Any further disclosure or dissemination of this document or the information contained herein is strictly prohibited without the approval of the Chicago Police Department's Crime Prevention & Information Center. Elements of this document may be subject to 28 CFR part 23. Illinois DL or ID images are only for use as authorized by 625 ILCS 5/6-110.1 and 92I11. Adm. Code 1030.140. This information shall not be released to the media or the general public. FAILURE TO ADHERE TO THESE POLICIES MAY RESULT IN CIVIL, CRIMINAL OR DISCIPLINARY ACTION.

It should be noted that some of this information describes First Amendment-protected activities. The Chicago Police Department's Crime Prevention and Information Center (CPIC) recognizes that Americans have constitutionally protected rights to assemble, speak, and petition the government. The CPIC safeguards these rights and only reports on First Amendment-protected activities for operational planning in the interest of assuring the safety and security of the demonstrators and the public. The CPIC will continue to communicate these events with other law enforcement partners in an effort to facilitate the Department's mission of assuring the safety and security of the demonstrators and the public.

(U//FOUO) IIB: Criminal Hackers Target US Law Enforcement Data, dated 29 June 2020

Sent: June 29, 2020 10:22:25 AM CDT
Received: June 29, 2020 10:26:08 AM CDT

FW: UNCLASS//FOUO//LES - Various Documents - June 29, 2020 - Part III

From:	Thomas Tilton (Emergency Management) <Thomas.Tilton@cookcountyil.gov>
To:	Michael Brady (Sheriff) <Michael.Brady@cookcountyil.gov>, Robert Lunk (Sheriff) <Robert.Lunk@cookcountyil.gov>
Sent:	June 29, 2020 11:21:15 AM CDT
Received:	June 29, 2020 11:21:21 AM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf, Anarchist Extremists - Antifa.pdf, Coronavirus Special OSINT Report - SOR 102-20.pdf, DMWA200629.pdf, OI Brief 29JUN20.pdf, Purple Notice 1002 - Concealment of cocaine (United Kingdom).pdf, SOUTHCOM Security Bulletin - 06.27.20.pdf, SWFO-IN Taking the Red Pill- Linguistic Indicators of Extremist Ideology.pdf, USBP NTC-BP BOLO 06-27-2020 Glenn Murray VANCIL (DoD).pdf, VILT Schedule Flyer - July 2020.pdf

Mike and Rob, I am on the mailing list of this group and I forward all of this product (and it is a LOT) everyday to our OIS people. Let me know if you guys like this. TT

From: Ness, Michael <michael.ness@hq.dhs.gov>
Sent: Monday, June 29, 2020 11:15 AM
To: Adrian Cunningham (Adrian.Cunningham@fema.dhs.gov); 'Adrianne.Michele@socom.mil'; AITES, KELLIE A CIV USAF ACC 55 SFS/S5AT <kellie.aites@us.af.mil>; 'Allen_Rothbaum@ios.doi.gov'; Anderson, Matthew E LT USN STRATCOM J34 (USA) (matthew.e.anderson5.mil@mail.mil) <matthew.e.anderson5.mil@mail.mil>; Distler, Andrew (CTR) <andrew.distler@associates.hq.dhs.gov>; MARCUS, ANDREW <andrew.marcus@hq.dhs.gov>; Anna Castillo <anna.castillo.1@us.af.mil>; Brad Tippit (Brad.Tippit@Missouricitytx.gov) <Brad.Tippit@Missouricitytx.gov>; 'Bruce.Steven.Miller@us.army.mil'; Pelton, Bryan (CTR) <bryan.pelton@associates.hq.dhs.gov>; 'captain@berwickpolice.org'; Chandra White <Chandra.white@us.af.mil>; Oppliger, Christopher <christopher.oppliger@hq.dhs.gov>; Cisneros, Tony <Tony.Cisneros@fletc.dhs.gov>; 'CLTibbs@co.pg.md.us'; ALFORD, DALE <dale.alford@hq.dhs.gov>; 'Darryl_Ward@ios.doi.gov'; ATWOOD, DAVID (CTR) <david.atwood@associates.hq.dhs.gov>; Davidson, Jeffrey <jeffrey.davidson@hq.dhs.gov>; Delcore, Robert <Robert.Delcore@uscis.dhs.gov>; Delgado, Jose L <Jose.Delgado@tsa.dhs.gov>; 'dennis.gonzalez@CityofRochester.gov'; dgirou@arlingtonva.us; 'dgpeterson@lanl.gov'; Schwarzrock, Don <don.schwarzrock@hq.dhs.gov>; Downey, Michael <Michael.Downey@hq.dhs.gov>; Dzurilla, Christopher <Christopher.Dzurilla@HQ.DHS.GOV>; Gagnon, Bruce P <Bruce_Gagnon@nps.gov>; Graves, Jeremy W MSgt USAF AFDW (USA) (jeremy.w.graves.mil@mail.mil) <jeremy.w.graves.mil@mail.mil>; greg.brock@nlrb.gov; HARDING, DANIEL <daniel.harding@hq.dhs.gov>; Harvey, Timothy <Timothy.Harvey@fletc.dhs.gov>; Henry Rivero: <Henry.Rivero@bep.gov>; 'hhgreen@nmic.navy.mil'; Holder, Richard <Richard.Holder@HQ.DHS.GOV>; Hughes, Gregory (CDC/OPHSS/NCHS) (nvx2@cdc.gov) <nvx2@cdc.gov>; Hunter, Joseph David (Joe) 2d LT USAF (US) (joseph.d.hunter16.mil@mail.mil) <joseph.d.hunter16.mil@mail.mil>; CURRIE, JASON (CTR) <jason.currie@associates.hq.dhs.gov>; Jeffrey McClung <jeffrey.mcclung@jfcc-imd.stratcom.mil>; Henderson, Jesse K CTR <Jesse.K.Henderson@uscg.mil>; Tadrick, Joe <Joe.Tadrick@hq.dhs.gov>; John Bamford <Jbamford@arlingtonva.us>; 'john.a.kavaliunas.civ@mail.mil'; 'John.Glodo@crystal.dia.mil'; 'john.leo-1@nasa.gov'; Jonesmcgee, Darius A SSgt USAF (USA) (darius.a.jonesmcgee.mil@mail.mil) <darius.a.jonesmcgee.mil@mail.mil>; JS Pentagon DoM Mailbox JSSO Military Security Force <js.pentagon.dom.mbx.jsso-military-security-force@mail.mil>; kenneth.j.anderson3.civ@mail.mil; Kristy KorchakCampbell (kristy.korchakcampbell@us.af.mil) <kristy.korchakcampbell@us.af.mil>; kristy.korchak-campbell@auab.afcent.af.mil; 'kunichs@guestservices.com'; Battiste, Lawrence <lawrence.battiste@hq.dhs.gov>; Lee Taylor (Lee.Taylor@hq.dhs.gov); Linneman, Eric <Eric.linneman@dla.mil>; Mannix, Alan <Alan.Mannix@bep.gov>; 'mark.holloway@ic.fbi.gov'; Marler, Christopher F SSgt USAF (USA) (christopher.f.marler.mil@mail.mil) <christopher.f.marler.mil@mail.mil>; Mascolo, John <John.Mascolo@tsa.dhs.gov>; 'Matthew.f.croson@usdoj.gov'; McBride, Chip <chip.mcbride@hq.dhs.gov>; Michael Malcolm <michael.s.malcolm2.civ@mail.mil>; Michael Robinson: <michael.robinson@bep.gov>; 'michael.g.copeland2.civ@mail.mil'; Michael.Kenny@bep.gov; 'michael.w.young8.ctr@mail.mil'; Mike Evans <Mike.Evans@calvertcountymd.gov>; monika.l.junker.civ@mail.mil; Moreta, Richard <richard.moreta@hq.dhs.gov>; Nicholas Paoletti (nicholas.paoletti.1@us.af.mil) <nicholas.paoletti.1@us.af.mil>; 'n-nc.peterson.ncj3.mbx.j34-letic-omb@mail.mil'; 'Odis.Stroud@cookcountyil.gov'; Oppermann, George Henry CIV USARMY USAG (US) <george.h.oppermann.civ@mail.mil>; Ortega, John A CIV <John.A.Ortega@uscg.mil>; Booker, Patrick M (N/A) <patrick.m.booker@uscis.dhs.gov>; Patterson, Richard V (Rick) CTR STRATCOM J34 (US)

<richard.v.patterson.ctr@mail.mil>; Pepin, Andrew <Andrew.Pepin@HQ.DHS.GOV>; Groven, Philip <Philip.Groven@hq.dhs.gov>; Ping, William Darion <william.d.ping.civ@mail.mil>; Pinkham, Lawrence H JR CIV STRATCOM J34 (US) <lawrence.h.pinkham.civ@mail.mil>; 'PittmanT@state.gov'; POULSEN, ROBERT A 2d Lt USAF ACC 55 ISS/IN <robert.poulsen@us.af.mil>; 'Raymond.Hankins@nlrb.gov'; Loveless, Richard <richard.loveless@hq.dhs.gov>; Richard Reed <Richard.Reed@firstnet.gov>; Richard Swarens <Richard.Swarens@whmo.mil>; 'Richard.Cestero@bep.gov'; Roddy, Gene E. CIV WHMO/HQ <Gene.E.Roddy@whmo.mil>; Russell, John W MSG USARMY JS DOM (US) <john.w.russell36.mil@mail.mil>; 'russell.r.hicks.civ@mail.mil'; BOYER, RYAN <ryan.boyer@hq.dhs.gov>; 'Ryan.Gibson@faa.gov'; 'Salvatore.ingraldi.civ@mail.mil'; Shell, Alvin <alvin.shell@bep.gov>; Sims, Karen <karen.sims@hq.doe.gov>; 'smithbr@state.gov'; Stephen J Barbieri (stephen.j.barbieri@uscis.dhs.gov); Stephen Kunich <Stephen.Kunich@pae.com>; 'Stephen.Hutchens@bep.gov'; Steven Schoen <steven.m.schoen@lmco.com>; Stewart, Kerry <Kerry.Stewart@cisa.dhs.gov>; Stewart, Kevin L CTR <Kevin.L.Stewart@uscg.mil>; 'sylvia.c.harris.civ@mail.mil'; Thomas Klug: <Thomas.Klug@bep.gov>; 'thomas.a.stroud@nasa.gov'; 'thomas.loyd@uscp.gov'; 'Thomas.Tilton@cookcountyil.gov'; Torian, William A Jr CIV USAF (USA) (william.a.torian.civ@mail.mil) <william.a.torian.civ@mail.mil>; Versichelli, Thomas <thomas.versichelli.civ@mail.mil>; Victor Calloway <vcalloway@gpo.gov>; Waage, Timothy S CIV STRATCOM J34 (US) <timothy.s.waage.civ@mail.mil>; Waterman, Ronald T CIV DSS DSS ISFO (US) <ronald.t.waterman.civ@mail.mil>; BERG, WENDY <wendy.berg@hq.dhs.gov>; WERNER, MATTHEW R TSgt USAF AFOSI 55 SFS/Det 204 <matthew.werner.4@us.af.mil>; Wilemon, Nicole <nwilemon@blm.gov>; DeArcangelis, William <william.dearcangelis@HQ.DHS.GOV>; Balcerzak, William J <William.J.Balcerzak@uscis.dhs.gov>; Wilson, Randall Craig CIV USARMY 21 SIG BDE (USA) (randall.c.wilson12.civ@mail.mil) <randall.c.wilson12.civ@mail.mil>; Wolf, Thomas John (Tom) CIV USARMY 21 SIG BDE (US) (thomas.j.wolf.civ@mail.mil) <thomas.j.wolf.civ@mail.mil>; Wyman, Isabel <isabel.wyman@hq.dhs.gov>
Subject: UNCLASS//FOUO//LES - Various Documents - June 29, 2020 - Part III

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Michael "Elliot" Ness
Program Manager
Industrial Security Branch – CCIPP Program Office
Office of Chief Security Officer | National Security Services Division |
DHS-HQ Desk: 202-447-5046 | Mobile Work Cell: 202-853-0569
Email(s): michael.ness@hq.dhs.gov, or OCSO-SARM@hq.dhs.gov

Homeland Security

"With honor and integrity, we will safeguard the American people, our homeland, and our values."

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator. This communication, along with any attachments, is covered by Federal and State law governing electronic communications and may contain restricted and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message.

From: McIntyre, Timothy A <Timothy.A.McIntyre@ice.dhs.gov>
Sent: Monday, June 29, 2020 11:33 AM
To: Ness, Michael <michael.ness@hq.dhs.gov>
Subject: (U/LES) Information

Timothy A. McIntyre, USN CPO Ret., MHS, CEM, CHS III
Security Specialist
U.S. Department of Homeland Security
U.S. Immigration and Customs Enforcement
Badge & Credential Program
One East Broad Street, Suite 200
Bethlehem, PA. 18018-5913
Office: (610) 861-8520 – Ext 107
Cell: (202) 277-2078
Fax: (610) 861-8525

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Paul Villanueva <paul.villanueva@cookcountyil.gov>, Paul Villanueva (Sheriff) <Paul.Villanueva@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:16:59 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Patrick Moriarty <Patrick.moriarty@cookcountyil.gov>, Patrick Moriarty (Sheriff) <Patrick.Moriarty@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:17:17 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Adam Murphy <adam.murphy@cookcountyil.gov>, Adam Murphy (Sheriff) <Adam.Murphy@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:16:27 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Phillip D Mackey <Phillip.mackey@cookcountyil.gov>, Phillip Mackey (Sheriff) <Phillip.Mackey@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:16:15 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Kathleen Urbanczyk <ccso.intel@cookcountyil.gov>, CCSO Intel (Sheriff) <CCSO.INTEL@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:19:50 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Timothy O'Donnell <Timothy.Odonnell@cookcountyil.gov>, Timothy O'Donnell (Sheriff) <Timothy.Odonnell@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:17:11 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Nicole Pagani <Nicole.Pagani@cookcountyil.gov>, Nicole Pagani (Sheriff) <Nicole.Pagani@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:16:54 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	darren.ganir@cookcountyil.gov, Darren Ganir (Sheriff) <Darren.Ganir@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:16:55 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Matthew Goral <matthew.goral@cookcountyil.gov>, Matthew Goral (Sheriff) <Matthew.Goral@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:19:36 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Ted Stajura <theodore.stajura@cookcountyil.gov>, Theodore Stajura (Sheriff) <Theodore.Stajura@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:17:06 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Robert A. Lunk <Robert.Lunk@cookcountyil.gov>, Robert Lunk (Sheriff) <Robert.Lunk@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:16:26 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	ginny.georgantas@cookcountyil.gov, Ginny Georgantas (Sheriff) <Ginny.Georgantas@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:17:41 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Sean chambers <Sean.chambers@cookcountyil.gov>, Sean Chambers (Sheriff) <Sean.Chambers@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:17:32 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Kate Schwendener <kathryn.schwendener@cookcountyil.gov>, Kathryn Schwendener (Sheriff) <Kathryn.Schwendener@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:18:16 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Craig A Wilk #747 <craig.wilk@cookcountyil.gov>, Craig Wilk (Sheriff) <Craig.Wilk@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:15:48 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Richard Brogan <Richard.brogan@cookcountyil.gov>, Richard Brogan (Sheriff) <Richard.Brogan@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:16:32 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	patrick.doyle@cookcountyil.gov, Patrick Doyle (Sheriff) <Patrick.Doyle@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:16:44 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Tarry Williams <Tarry.williams@cookcountyil.gov>, Tarry Williams (Sheriff) <Tarry.Williams@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:17:10 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	John Konrad <john.konrad@cookcountyil.gov>, John Konrad (Sheriff) <John.Konrad@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:16:11 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	Jerome Ryan <jerome.ryan@cookcountyil.gov>, Jerome Ryan (Sheriff) <Jerome.Ryan@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:16:17 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	ISP.DoNotReply <ISP.DoNotReply@Illinois.gov>
To:	peter.pon@cookcountyil.gov, Peter Pon (Sheriff) <Peter.Pon@cookcountyil.gov>
Sent:	June 29, 2020 3:12:35 PM CDT
Received:	June 29, 2020 3:16:55 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Patrick Moriarty (Sheriff)
Sent: June 29, 2020 3:12:35 PM CDT
Received: June 29, 2020 3:17:18 PM CDT

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Phillip Mackey (Sheriff)
Sent: June 29, 2020 3:12:35 PM CDT
Received: June 29, 2020 3:16:18 PM CDT

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Theodore Stajura (Sheriff)
Sent: June 29, 2020 3:12:35 PM CDT
Received: June 29, 2020 3:17:06 PM CDT

(U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Craig Wilk (Sheriff)
Sent: June 29, 2020 3:12:35 PM CDT
Received: June 29, 2020 3:15:48 PM CDT

FW: (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Sheriff Intel
Sent: June 29, 2020 3:19:50 PM CDT
Received: June 29, 2020 3:19:53 PM CDT

FW: (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	Kathleen Urbanczyk (Sheriff) <Kathleen.Urbanczyk@cookcountyil.gov>
To:	Kathryn Schwendener (Sheriff) <Kathryn.Schwendener@cookcountyil.gov>
Sent:	June 29, 2020 3:25:50 PM CDT
Received:	June 29, 2020 3:25:51 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

From: CCSO Intel (Sheriff) <CCSO.INTEL@cookcountyil.gov>
Sent: Monday, June 29, 2020 3:20 PM
To: Sheriff Intel <sheriff.intel@cookcountyil.gov>
Subject: FW: (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From: ISP.DoNotReply
Sent: Monday, June 29, 2020 3:12:35 PM (UTC-06:00) Central Time (US & Canada)
To: CCSO Intel (Sheriff)
Subject: (U//FOUO) Criminal Hackers Target US Law Enforcement Data

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

FW: (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	Kathleen Urbanczyk (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=AAE0F208D8C54334A96AA19F2B1E4048-KATHLEEN UR>
To:	Kathryn Schwendener (Sheriff) <Kathryn.Schwendener@cookcountyil.gov>
Sent:	June 29, 2020 3:25:50 PM CDT
Received:	June 29, 2020 3:25:00 PM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

From: CCSO Intel (Sheriff) <CCSO.INTEL@cookcountyil.gov>
Sent: Monday, June 29, 2020 3:20 PM
To: Sheriff Intel <sheriff.intel@cookcountyil.gov>
Subject: FW: (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From: ISP.DoNotReply
Sent: Monday, June 29, 2020 3:12:35 PM (UTC-06:00) Central Time (US & Canada)
To: CCSO Intel (Sheriff)
Subject: (U//FOUO) Criminal Hackers Target US Law Enforcement Data

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

The following information is being disseminated by STIC to our email distribution list for situational awareness purposes. Replies can be sent to stic@illinois.gov.

Good afternoon,

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

FW: (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Kathryn Schwendener (Sheriff)
Sent: June 29, 2020 3:25:50 PM CDT
Received: June 29, 2020 3:25:00 PM CDT

Good Cyber Hygiene in a Post COVID World | Average Cost of a Data Breach: $116M | 5 Steps for Implementing Multicloud Identity

From: Information Management Today Weekly <editors@aggregage.com>
To: Keith Morrison <keith.morrison@cookcountyil.gov>, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: June 29, 2020 9:28:49 PM CDT
Received: June 29, 2020 9:28:58 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Top articles on Security and Government.

Edition: Week of Jun 20, 2020

Information Management Today
Expert insights. Personalized for you.

Brought to you by

Trending Articles:

Pressure Points: How to Ensure Your B2B Pipeline Passes Inspection

This eBook highlights best practices for developing a pipeline management process that helps sales leaders and their team C.L.O.S.E (you'll see what we mean in this eBook) more revenue through data-driven prospecting, stage analysis, and subsequent sales enablement.

ADVERTISER: ZOOMINFO

Future-Proofing Your Information Governance Strategy

Join Onna and experts from Quip, Airbnb, and Oracle for this recorded webinar as they dive into proactive data deletion policies, retention strategies, and legal hold practices that are essential to a modern enterprise information governance strategy.

ADVERTISER: ONNA

Good Cyber Hygiene in a Post-Pandemic World Starts with Us

Three ways that security teams can improve processes and collaboration, all while creating the common ground needed to sustain them

DARK READING

Average Cost of a Data Breach: $116M

Sensitivity of customer information and time-to-detection determine financial blowback of cybersecurity breaches

DARK READING

5 Steps for Implementing Multicloud Identity

Why embracing, not fighting, decentralization will pave the way to smoother cloud migrations

DARK READING

Check out the full edition!

Picked For You:

US Now Accuses Assange of Conspiring With Hacking Groups

Superseding Indictment Expands Scope of Case, But Doesn't Add Charges The U.S Department of Justice unsealed a superseding indictment against WikiLeaks founder Julian Assange that expands the scope of the government's case against him.

DATA BREACH TODAY

‘BlueLeaks’ Exposes Files from Hundreds of Police Departments

Hundreds of thousands of potentially sensitive files from police departments across the United States were leaked online last week. The collection, dubbed “ BlueLeaks ” and made searchable online, stems from a security breach at a Texas web design and hosting company that maintains a number of state law enforcement data-sharing portals.

KREBS ON SECURITY

MY TAKE: Remote classes, mobile computing heighten need for a security culture in K-12 schools

Parents have long held a special duty to protect their school-aged children from bad actors on the Internet. Related: Mock attacks help schools defend themselves Now COVID-19 has dramatically and permanently expanded that parental responsibility, as well as extended it to ill-prepared school officials in K-12 campuses all across the nation.

THE LAST WATCHDOG

More Trending:

Anonymous Stole and Leaked a Megatrove of Police Documents

The so-called BlueLeaks collection includes internal memos, financial records, and more from over 200 state, local, and federal agencies. Security Security / Cyberattacks and Hacks

WIRED THREAT LEVEL

Nephilim Ransomware Gang Tied to Citrix Gateway Hacks

DATA BREACH TODAY

New Charges, Sentencing in Satori IoT Botnet Conspiracy

The U.S. Justice Department today criminally charged a Canadian and a Northern Ireland man for allegedly conspiring to build botnets that enslaved hundreds of thousands of routers and other Internet of Things (IoT) devices for use in large-scale distributed denial-of-service (DDoS) attacks.

KREBS ON SECURITY

Click here to see this edition in full, including:

SHARED INTEL: How ransomware evolved from consumer trickery to deep enterprise hacks
THE LAST WATCHDOG

Developer of DDoS Mirai based botnets sentenced to prison
PIERLUIGI PAGANINI

Breach Notification Delay: A Step-by-Step Timeline
DATA BREACH TODAY

5 New InfoSec Job Training Trends: What We're Studying During COVID-19
DARK READING

COVID-19 Risks of Flying

SCHNEIER ON SECURITY

Akamai mitigated the largest ever PPS DDoS attack

SECURITY AFFAIRS

Payment Card Skimmer Attacks Hit 8 Cities

An Embattled Group of Leakers Picks Up the WikiLeaks Mantle

WIRED THREAT LEVEL

Cybercrime Infrastructure Never Really Dies

DARK READING

Moroccan journalist targeted with network injection attacks using NSO Group ‘s spyware

SECURITY AFFAIRS

Check out the full edition!

Copyright 2020 | Aggregage | 525 South Douglas Ave, Suite 260 | El Segundo, CA 90245 USA. Email sent to keith.morrison@cookcountyil.gov. To stop receiving emails at this address manage your subscription or unsubscribe.
Powered by Aggregage - expert insights. personalized for you.. Forward this email to a friend!

[GovQA] FOIA Request - New Assignment - R009142-062920

From: Cook County Sheriff's Office <cookcountysheriff@govqa.us>
To: Elizabeth.Scannell@cookcountyil.gov, Elizabeth Scannell (Sheriff) <Elizabeth.Scannell@cookcountyil.gov>
Sent: June 30, 2020 7:56:10 AM CDT
Received: June 30, 2020 7:56:13 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

A request has been assigned to you: FOIA Request / R009142-062920

FOIA Request for Records
Assigned Staff: Elizabeth Scannell
Status: Received
Create Date: June 29, 2020
Due Date: July 06, 2020
Name of Requester: Emma Best
Requester Affiliation: Press
Record(s) Requested: To Whom It May Concern: Pursuant to the Illinois Freedom of Information Act., I hereby request the following records: 1. Documents mentioning, describing or generated in response to the BlueLeaks release, the preceding hack or subsequent fallout, including but not limited to: * Damage assessments * Emails * Interagency communications (local, state, or federal) * Communications with the press about BlueLeaks * Communications with Twitter or other social media or sharing platforms 2. Documents mentioning or describing Distributed Denial of Secrets (DDoSecrets) You may limit this request to records generated between November 1, 2018 and the present. I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers in outlets such as Gizmodo, MuckRock, Motherboard, Property of the People, Unicorn Riot, and The Outline, among others. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the library Internet Archive and the journalist non-profit MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself. As such, it is not necessary for me to demonstrate the relevance of this particular subject in advance. As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived. The requested documents will be made available to the general public, and this request is not being made for commercial purposes. In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not. Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 5 business days, as the statute requires. Sincerely, Emma Best Upload documents directly: https://https://www.muckrock.comhttps://accounts.muckrock.com/accounts/login/?next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fcook-county-sheriff-719%252Fblueleaks-cook-county-sheriff-96941%252F%253F&url_auth_token=AAAaaJnszUVssmdgx6fh2R-tE3U%3A1jppAE%3ADWZbgy7n864OATjAMxtAsPZltYs

Login to the system and view your request by clicking HERE. Your username and password is the same as your Active Directory login, used to access all CCSO computers. If you have any questions or concerns regarding this email notification, please contact the Legal Department at 312-603-6444.

This is an auto-generated email and has originated from an unmonitored email account. Please DO NOT REPLY to this email as the contents of your response and any attachments may be externally disseminated inadvertently. Click the link above to respond and upload documents for secure internal review.

Emma Best FOIA R009142-062920

From:	Eryn Hedderman (Sheriff) <Eryn.Hedderman@cookcountyil.gov>
To:	Elizabeth Scannell (Sheriff) <Elizabeth.Scannell@cookcountyil.gov>
Sent:	June 30, 2020 7:58:48 AM CDT
Received:	June 30, 2020 7:58:49 AM CDT
Attachments:	FOIA R009142-062920.pdf

Hello!

We received the attached FOIA request from Emma Best, including emails. I have assigned this for you on GovQA.

Thank you,

Eryn Hedderman
Cook County Sheriff's Office
FOIA Support/Legal Department

The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential and may be subject to applicable attorney-client and/or work product privileges. If you are not the intended recipient of this message or if this message has been addressed to you in error, please alert the sender immediately by reply e-mail and then delete this message and its attachments. Do not deliver, distribute or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action in reliance upon the information contained in this communication or any attachments. Thank you.

Emma Best FOIA R009142-062920

From:	Eryn Hedderman (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DA84F6C14E4A40FFB4B4B24D87E04CEF-ERYN T. HED>
To:	Elizabeth Scannell (Sheriff) <Elizabeth.Scannell@cookcountyil.gov>
Sent:	June 30, 2020 7:58:48 AM CDT
Received:	June 30, 2020 7:58:00 AM CDT
Attachments:	FOIA R009142-062920.pdf

Hello!

We received the attached FOIA request from Emma Best, including emails. I have assigned this for you on GovQA.

Thank you,

Eryn Hedderman
Cook County Sheriff's Office
FOIA Support/Legal Department

The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential and may be subject to applicable attorney-client and/or work product privileges. If you are not the intended recipient of this message or if this message has been addressed to you in error, please alert the sender immediately by reply e-mail and then delete this message and its attachments. Do not deliver, distribute or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action in reliance upon the information contained in this communication or any attachments. Thank you.

Emma Best FOIA R009142-062920

To:	Elizabeth Scannell (Sheriff)
Sent:	June 30, 2020 7:58:48 AM CDT
Received:	June 30, 2020 7:58:00 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

Sent: June 30, 2020 8:06:39 AM CDT
Received: June 30, 2020 8:06:47 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Sheriff Intel
Sent: June 30, 2020 8:06:39 AM CDT
Received: June 30, 2020 8:06:48 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Sheriff Intel, Paul Villanueva (Sheriff)
Sent:	June 30, 2020 8:06:39 AM CDT
Received:	June 30, 2020 8:06:47 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Michael Rowe (Sheriff)
Sent: June 30, 2020 8:06:39 AM CDT
Received: June 30, 2020 8:06:48 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: George Winistorfer (Sheriff)
Sent: June 30, 2020 8:06:39 AM CDT
Received: June 30, 2020 8:06:48 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Anastasios Goulos (Sheriff)
Sent: June 30, 2020 8:06:39 AM CDT
Received: June 30, 2020 8:06:47 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Ricky Soto (Sheriff)
Sent:	June 30, 2020 8:06:39 AM CDT
Received:	June 30, 2020 8:06:47 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Nicole Pagani (Sheriff)
Sent:	June 30, 2020 8:06:39 AM CDT
Received:	June 30, 2020 8:06:48 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Darren Ganir (Sheriff)
Sent:	June 30, 2020 8:06:39 AM CDT
Received:	June 30, 2020 8:06:47 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Amar Patel (Sheriff), Keith Morrison (Sheriff), Adnan Memon (Sheriff), Douglas Maclean (Sheriff)
Cc:	Adnan Memon (Sheriff), Douglas Maclean (Sheriff), Amar Patel (Sheriff)
Sent:	June 30, 2020 8:06:39 AM CDT
Received:	June 30, 2020 8:06:48 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Sheriff Intel, Sean Chambers (Sheriff)
Sent:	June 30, 2020 8:06:39 AM CDT
Received:	June 30, 2020 8:06:47 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Kathryn Schwendener (Sheriff), Sheriff Intel
Sent:	June 30, 2020 8:06:39 AM CDT
Received:	June 30, 2020 8:06:48 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Neal Gaynor (Sheriff)
Sent:	June 30, 2020 8:06:39 AM CDT
Received:	June 30, 2020 8:06:47 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Richard Brogan (Sheriff)
Sent:	June 30, 2020 8:06:39 AM CDT
Received:	June 30, 2020 8:06:48 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Jazmond Watson (Sheriff)
Sent: June 30, 2020 8:06:39 AM CDT
Received: June 30, 2020 8:06:48 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Carl Price (Sheriff)
Sent:	June 30, 2020 8:06:39 AM CDT
Received:	June 30, 2020 8:06:47 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Peter Pon (Sheriff)
Sent:	June 30, 2020 8:06:39 AM CDT
Received:	June 30, 2020 8:06:48 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From: CCSO Intel (Sheriff) <CCSO.INTEL@cookcountyil.gov>

Bcc: 911 Telecommunicators <All_911_Center@cookcountyil.gov>, Aaron Spears (Sheriff) <Aaron.Spears@cookcountyil.gov>, Abraham Yasin (Sheriff) <Abraham.Yasin@cookcountyil.gov>, Amanda Ruzich (Sheriff) <Amanda.Ruzich@cookcountyil.gov>, Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Anastasios Goulos (Sheriff) <Anastasios.Goulos@cookcountyil.gov>, Andre Bonhart (Sheriff) <Andre.Bonhart@cookcountyil.gov>, Angel Nieves (Sheriff) <Angel.Nieves@cookcountyil.gov>, Anthony Colquitt (Sheriff) <Anthony.Colquitt@cookcountyil.gov>, Anthony Del Santo (Sheriff) <Anthony.DelSanto@cookcountyil.gov>, Ashley O'Connor (Sheriff) <Ashley.O'Connor@cookcountyil.gov>, Barbaro Chang (Sheriff) <Barbaro.Chang@cookcountyil.gov>, Bradley M Curry (Sheriff) <Bradley.Curry@cookcountyil.gov>, Brenda Humphrey (Sheriff) <Brenda.Humphrey@cookcountyil.gov>, Brenda Merle (Sheriff) <Brenda.Merle@cookcountyil.gov>, Brian Bialczak (Sheriff) <Brian.Bialczak@cookcountyil.gov>, Brian Gibbs (Sheriff) <Brian.Gibbs@cookcountyil.gov>, Brian Olano (Sheriff) <Brian.Olano@cookcountyil.gov>, Carmen Gercone (Sheriff) <Carmen.Gercone@cookcountyil.gov>, Carole Collins (Sheriff) <Carole.Collins@cookcountyil.gov>, Cathy Geraghty (Forest Preserve District) <cathy.geraghty@cookcountyil.gov>, Charmaine Charmelo (Sheriff) <Charmaine.Charmelo@cookcountyil.gov>, Chris Kaloudis (Sheriff) <Chris.Kaloudis@cookcountyil.gov>, Constantine Jovica (Sheriff) <Constantine.Jovica@cookcountyil.gov>, Cynthia Sorrentino (Sheriff) <Cynthia.Sorrentino@cookcountyil.gov>, Daniel Cramer (Sheriff) <Daniel.Cramer@cookcountyil.gov>, Daniel Gutierrez (Sheriff) <Daniel.Gutierrez@cookcountyil.gov>, Daniel Moreci (Sheriff) <Daniel.Moreci@cookcountyil.gov>, Darren Ganir (Sheriff) <Darren.Ganir@cookcountyil.gov>, Darren Makowski (Sheriff) <Darren.Makowski@cookcountyil.gov>, Darren Rycyzyn (Sheriff) <Darren.Rycyzyn@cookcountyil.gov>, Daryl Howell (Sheriff) <Daryl.Howell@cookcountyil.gov>, David Booker (Sheriff) <David.Booker@cookcountyil.gov>, David Chiko (Sheriff) <David.Chiko@cookcountyil.gov>, Dawn Guerrero (Sheriff) <Dawn.Guerrero@cookcountyil.gov>, Debbie Boecker (Sheriff) <Debbie.Boecker@cookcountyil.gov>, Denise Klueg (Sheriff) <Denise.Klueg@cookcountyil.gov>, Dennis Nicpan (Sheriff) <Dennis.Nicpan@cookcountyil.gov>, Doris Banks-Harrison (Sheriff) <Doris.Banks-Harrison@cookcountyil.gov>, Drake Carpenter (Sheriff) <Drake.Carpenter@cookcountyil.gov>, Edward Pickell (Sheriff) <Edward.Pickell@cookcountyil.gov>, Elizabeth Potter (Sheriff) <Elizabeth.Potter@cookcountyil.gov>, Eric Mills (Sheriff) <Eric.Mills@cookcountyil.gov>, Erica Queen (Sheriff) <Erica.Queen@cookcountyil.gov>, Esther Montanez (Sheriff) <Esther.Montanez@cookcountyil.gov>, George Winistorfer (Sheriff) <George.Winistorfer@cookcountyil.gov>, Georgia Garcia (Sheriff) <Georgia.Garcia@cookcountyil.gov>, Geraldo Medina (Sheriff) <Geraldo.Medina@cookcountyil.gov>, Gloria Guerrero (Sheriff) <Gloria.Guerrero@cookcountyil.gov>, Gregory Ernst (Sheriff) <Gregory.Ernst@cookcountyil.gov>, Grisel Nava (Sheriff) <Grisel.Nava@cookcountyil.gov>, Henry Hemphill (Sheriff) <Henry.Hemphill@cookcountyil.gov>, Henry McNally (Sheriff) <Henry.Mcnally@cookcountyil.gov>, Hugh Walsh (Sheriff) <Hugh.Walsh@cookcountyil.gov>, Ivette Perez (Sheriff) <Ivette.Perez@cookcountyil.gov>, Jacqueline Manna (Sheriff) <Jacqueline.Manna@cookcountyil.gov>, Jaimee Kapolnek (Sheriff) <Jaimee.Kapolnek@cookcountyil.gov>, James Dillon (Sheriff) <James.Dillon@cookcountyil.gov>, JAMES ROACHE (States Attorney) <JAMES.ROACHE@cookcountyil.gov>, James Siroky (Sheriff)

<James.Siroky@cookcountyil.gov>, Janet Kostanski (Sheriff)
<Janet.Kostanski@cookcountyil.gov>, Jeff Johnsen (Sheriff)
<Jeff.Johnsen@cookcountyil.gov>, Jeremy Corning (Sheriff)
<Jeremy.Corning@cookcountyil.gov>, JoAnn Abruzzo (Sheriff)
<JoAnn.Abruzzo@cookcountyil.gov>, John Cornier (Sheriff)
<John.Cornier@cookcountyil.gov>, John Hammond (Sheriff)
<John.Hammond@cookcountyil.gov>, John Harrington (Sheriff)
<John.Harrington@cookcountyil.gov>, John Norton (Sheriff)
<John.Norton@cookcountyil.gov>, John O'Farrell (Sheriff)
<John.Ofarrell@cookcountyil.gov>, John Scarpelli (Sheriff)
<John.Scarpelli@cookcountyil.gov>, Jonathan Myslinski (Sheriff)
<Jonathan.Myslinski@cookcountyil.gov>, Jose Medina (Sheriff)
<Jose.Medina@cookcountyil.gov>, Joseph Bellettiere (Sheriff)
<Joseph.Bellettiere@cookcountyil.gov>, Joseph Boyle (Sheriff)
<Joseph.Boyle@cookcountyil.gov>, Joseph Giunta (Sheriff)
<Joseph.Giunta@cookcountyil.gov>, Joseph Ryan1 (Sheriff)
<Joseph.Ryan2@cookcountyil.gov>, Joseph Spain (Sheriff)
<Joseph.Spain@cookcountyil.gov>, Joseph Younan (Sheriff)
<Joseph.Younan@cookcountyil.gov>, Juan Diaz (Sheriff)
<Juan.Diaz@cookcountyil.gov>, Juan Salinas (Sheriff)
<Juan.Salinas@cookcountyil.gov>, Kathleen Kirby (Sheriff)
<Kathleen.Kirby@cookcountyil.gov>, Kathleen Urbanczyk (Sheriff)
<Kathleen.Urbanczyk@cookcountyil.gov>, Kenneth Radermacher (Sheriff)
<Kenneth.Radermacher@cookcountyil.gov>, Kevin Connelly (Sheriff)
<Kevin.Connelly@cookcountyil.gov>, Kimberly Hofsteadter (Sheriff)
<Kimberly.Hofsteadter@cookcountyil.gov>, Kimberly Stein (Sheriff)
<Kimberly.Stein@cookcountyil.gov>, Kyle Halvorson (Sheriff)
<Kyle.Halvorson@cookcountyil.gov>, Larry Schurig (Sheriff)
<Larry.Schurig@cookcountyil.gov>, Laura Corrado (Sheriff)
<Laura.Corrado@cookcountyil.gov>, Lawrence Ostrowski (Sheriff)
<Lawrence.Ostrowski@cookcountyil.gov>, Lawrence Weston (Sheriff)
<Lawrence.Weston@cookcountyil.gov>, Lee Ringler (Sheriff)
<Lee.Ringler@cookcountyil.gov>, Leonard Jagielski (Sheriff)
<Leonard.Jagielski@cookcountyil.gov>, Leroy Martiniak (Sheriff)
<Leroy.Martiniak@cookcountyil.gov>, Liz Glick (Sheriff)
<Liz.Glick@cookcountyil.gov>, Mariel Ramirez (Sheriff)
<Mariel.Ramirez@cookcountyil.gov>, Mark Modert (Sheriff)
<Mark.Modert@cookcountyil.gov>, Mary Downes (Sheriff)
<Mary.Downes@cookcountyil.gov>, Mary McQuillan (Sheriff)
<Mary.Mcquillan@cookcountyil.gov>, Matthew Cobble (Sheriff)
<Matthew.Cobble@cookcountyil.gov>, Matthew Jaeky (Sheriff)
<Matthew.Jaeky@cookcountyil.gov>, Maureen Wasco (Sheriff)
<Maureen.Wasco@cookcountyil.gov>, Melissa Perez (Sheriff)
<Melissa.Perez@cookcountyil.gov>, Michael Brady (Sheriff)
<Michael.Brady@cookcountyil.gov>, Michael Carbone (Sheriff)
<Michael.Carbone2@cookcountyil.gov>, Michael Fitzpatrick (Sheriff)
<Michael.Fitzpatrick@cookcountyil.gov>, Michael Flamburis (Sheriff)
<Michael.Flamburis@cookcountyil.gov>, Michael Grady (Sheriff)
<Michael.Grady@cookcountyil.gov>, Michael Keane (Juvenile Probation)
<michael.keane@cookcountyil.gov>, Michael Knighton (Sheriff)
<Michael.Knighton@cookcountyil.gov>, Michael Manade (Sheriff)
<Michael.Manade@cookcountyil.gov>, Michael Mc Hugh (Sheriff)
<Michael.McHugh2@cookcountyil.gov>, Michael Miller (Sheriff)
<Michael.Miller1@cookcountyil.gov>, Michael Reed (Sheriff)
<Michael.Reed2@cookcountyil.gov>, Michael Sheehan (Sheriff)
<Michael.Sheehan@cookcountyil.gov>, Mike Vallejo (Sheriff)
<Mike.Vallejo@cookcountyil.gov>, Miles Cooperman (Sheriff)
<Miles.Cooperman@cookcountyil.gov>, Miriam Rentas (Sheriff)
<Miriam.Rentas@cookcountyil.gov>, Natalie Camer (Sheriff)
<Natalie.Camer@cookcountyil.gov>, Nicholas Margarites (Sheriff)
<Nicholas.Margarites@cookcountyil.gov>, Nicole Pagani (Sheriff)
<Nicole.Pagani@cookcountyil.gov>, Nicole Rafferty (Sheriff)
<Nicole.Rafferty@cookcountyil.gov>, Patrick Bradley (Sheriff)

<Patrick.Bradley@cookcountyil.gov>, Patrick Fitzgerald (Sheriff)
<Patrick.Fitzgerald@cookcountyil.gov>, Patrick Flannery (Sheriff)
<Patrick.Flannery@cookcountyil.gov>, Patrick Hecker (Sheriff)
<Patrick.Hecker@cookcountyil.gov>, Patrick Moerlien (Sheriff)
<Patrick.Moerlien@cookcountyil.gov>, Paul Kimbrough (Sheriff)
<Paul.Kimbrough@cookcountyil.gov>, Paul Villanueva (Sheriff)
<Paul.Villanueva@cookcountyil.gov>, Paul Worthon (Sheriff)
<Paul.Worthon@cookcountyil.gov>, Peter Pon (Sheriff)
<Peter.Pon@cookcountyil.gov>, Phillip Mackey (Sheriff)
<Phillip.Mackey@cookcountyil.gov>, Randall Haber (Sheriff)
<Randall.Haber@cookcountyil.gov>, Rashanda Carroll (Sheriff)
<Rashanda.Carroll@cookcountyil.gov>, Raymond Hash (Sheriff)
<Raymond.Hash@cookcountyil.gov>, Richard Brogan (Sheriff)
<Richard.Brogan@cookcountyil.gov>, Richard Ellitch (Sheriff)
<Richard.Ellitch@cookcountyil.gov>, Richard Kim (Sheriff)
<Richard.Kim@cookcountyil.gov>, Richard O'Brien (Sheriff)
<Richard.OBrien1@cookcountyil.gov>, Richard Young (Sheriff)
<Richard.Young2@cookcountyil.gov>, Ricky Soto (Sheriff)
<Ricky.Soto@cookcountyil.gov>, Robert Bonakowski (Sheriff)
<Robert.Bonakowski@cookcountyil.gov>, Robert Byrnes (Sheriff)
<Robert.Byrnes@cookcountyil.gov>, Robert Mazza (Sheriff)
<Robert.Mazza@cookcountyil.gov>, Robert Reilly (Sheriff)
<Robert.Reilly@cookcountyil.gov>, Rose Kane (Sheriff)
<Rose.Kane@cookcountyil.gov>, Rotonda Malone-Cole (Sheriff)
<Rotonda.Malone-Cole@cookcountyil.gov>, Ryan Killacky (Sheriff)
<Ryan.Killacky@cookcountyil.gov>, Salomon Martinez (Sheriff)
<Salomon.Martinez@cookcountyil.gov>, Samantha Thompson (Sheriff)
<Samantha.Thompson@cookcountyil.gov>, Samuel Cuellar (Sheriff)
<Samuel.Cuellar@cookcountyil.gov>, Sandra Antczak (Sheriff)
<Sandra.Antczak@cookcountyil.gov>, Alexander Chew (Sheriff)
<Alexander.Chew@cookcountyil.gov>, Parris Williams (Sheriff)
<Parris.Williams@cookcountyil.gov>, Adriana Morales (Sheriff)
<Adriana.Morales@cookcountyil.gov>, Deidre Williams (Sheriff)
<Deidre.Williams@cookcountyil.gov>, James Dolehide (Sheriff)
<James.Dolehide@cookcountyil.gov>, Kathryn Schwendener (Sheriff)
<Kathryn.Schwendener@cookcountyil.gov>, Timothy Kaufmann (Sheriff)
<Timothy.Kaufmann@cookcountyil.gov>, Cynthia Lance (Forest Preserve District) <Cynthia.Lance@cookcountyil.gov>, Kelvin Pope (Forest Preserve District) <Kelvin.Pope@cookcountyil.gov>, Besart Mila (Sheriff)
<Besart.Mila@cookcountyil.gov>, Andrew Hein (Sheriff)
<Andrew.Hein@cookcountyil.gov>, Alan Kickert (Sheriff)
<Alan.Kickert@cookcountyil.gov>, Daniel Lakowski (Sheriff)
<Daniel.Lakowski@cookcountyil.gov>, Collin McArdle (Sheriff)
<Collin.McArdle@cookcountyil.gov>, Clifford Brazzille (Sheriff)
<Clifford.Brazzille@cookcountyil.gov>, Christopher Suggs (Sheriff)
<Christopher.Suggs@cookcountyil.gov>, Brian Nyberg (Sheriff)
<Brian.Nyberg@cookcountyil.gov>, Brian Ashe (Sheriff)
<Brian.Ashe@cookcountyil.gov>, Joseph Danzl (Sheriff)
<Joseph.Danzl@cookcountyil.gov>, John Bennett (Sheriff)
<John.Bennett@cookcountyil.gov>, Jazmond Watson (Sheriff)
<Jazmond.Watson@cookcountyil.gov>, Jason McCall (Sheriff)
<Jason.McCall@cookcountyil.gov>, Jason Cianciarulo (Sheriff)
<Jason.Cianciarulo@cookcountyil.gov>, Jasmina Janjic (Sheriff)
<Jasmina.Janjic@cookcountyil.gov>, Israel Malave (Sheriff)
<Israel.Malave@cookcountyil.gov>, Felix Hernandez (Sheriff)
<Felix.Hernandez@cookcountyil.gov>, Fabio Valentini (Sheriff)
<Fabio.Valentini2@cookcountyil.gov>, Evan Fermaint (Sheriff)
<Evan.Fermaint@cookcountyil.gov>, Eric Schroeder (Sheriff)
<Eric.Schroeder@cookcountyil.gov>, Michael Falardeau (Sheriff)
<Michael.Falardeau@cookcountyil.gov>, Michael Bennett (Sheriff)
<Michael.Bennett@cookcountyil.gov>, Maurice Ashford (Sheriff)
<Maurice.Ashford@cookcountyil.gov>, Maureen Malloy (Sheriff)
<Maureen.Malloy@cookcountyil.gov>, Kevin Suchocki (Sheriff)

<Kevin.Suchocki@cookcountyil.gov>, Judie Sell (Sheriff)
<Judie.Sell@cookcountyil.gov>, Patrick Noonan (Sheriff)
<Patrick.Noonan@cookcountyil.gov>, Patrick Kaminski (Sheriff)
<Patrick.Kaminski@cookcountyil.gov>, Nicole Valerio (Sheriff)
<Nicole.Valerio@cookcountyil.gov>, Neal Creamer (Sheriff)
<Neal.Creamer@cookcountyil.gov>, Miriam Santiago (Sheriff)
<Miriam.Santiago@cookcountyil.gov>, Michael Rowe (Sheriff)
<Michael.Rowe@cookcountyil.gov>, Steven Valenza (Sheriff)
<Steven.Valenza@cookcountyil.gov>, Steven Martino (Sheriff)
<Steven.Martino@cookcountyil.gov>, Steve Jirgal (Sheriff)
<Steve.Jirgal@cookcountyil.gov>, Stephen Bouffard (Sheriff)
<Stephen.Bouffard@cookcountyil.gov>, Stephan Maglaya (Sheriff)
<Stephan.Maglaya@cookcountyil.gov>, Shahid Shekha (Sheriff)
<Shahid.Shekha@cookcountyil.gov>, Sergio Cervantes (Sheriff)
<Sergio.Cervantes@cookcountyil.gov>, Sean Chambers (Sheriff)
<Sean.Chambers@cookcountyil.gov>, Scott Guzik (Sheriff)
<Scott.Guzik@cookcountyil.gov>, Richard Liboy (Sheriff)
<Richard.Liboy@cookcountyil.gov>, Reginald Barker (Sheriff)
<Reginald.Barker@cookcountyil.gov>, Perry Triveri (Sheriff)
<Perry.Triveri@cookcountyil.gov>, Timothy Blake (Sheriff)
<Timothy.Blake@cookcountyil.gov>, Tia Parks-Jefferson (Sheriff) <Tia.Parks-Jefferson@cookcountyil.gov>, Thomas Ryan (Sheriff)
<Thomas.Ryan2@cookcountyil.gov>, Thomas Brunet (Sheriff)
<Thomas.Brunet@cookcountyil.gov>, Tarry Williams (Sheriff)
<Tarry.Williams@cookcountyil.gov>, Steven Williams (Sheriff)
<Steven.Williams@cookcountyil.gov>, Victoria Winford (Sheriff)
<Victoria.Winford@cookcountyil.gov>, Victoria Haig (Sheriff)
<Victoria.Haig@cookcountyil.gov>, Valerie Spurlock (Sheriff)
<Valerie.Spurlock@cookcountyil.gov>, Valerie Koedyker (Sheriff)
<Valerie.Koedyker@cookcountyil.gov>, Tracy Cavanaugh (Sheriff)
<Tracy.Cavanaugh@cookcountyil.gov>, Timothy Cook (Sheriff)
<Timothy.Cook@cookcountyil.gov>, Zelda Whittler (Sheriff)
<Zelda.Whittler@cookcountyil.gov>, William Shepski-Lindsted (Sheriff)
<William.Shepski-Lindsted@cookcountyil.gov>, William Scanlon (Sheriff)
<William.Scanlon@cookcountyil.gov>, William Behenna (Sheriff)
<William.Behenna@cookcountyil.gov>, Wanda Gastile (Sheriff)
<Wanda.Gastile@cookcountyil.gov>, CCSO EM
<ccso.em@cookcountyil.gov>, Eyman Zabadneh (Sheriff)
<Eyman.Zabadneh@cookcountyil.gov>, Stefana Castillo (Sheriff)
<Stefana.Castillo@cookcountyil.gov>, Adnan Memon (Sheriff)
<Adnan.Memon@cookcountyil.gov>, Douglas Maclean (Sheriff)
<Douglas.Maclean2@cookcountyil.gov>, Nikolas Hadjian (Sheriff)
<Nikolas.Hadjian@cookcountyil.gov>, Michael Bernardini (Juvenile Temporary Detention Center) <Michael.Bernardini@cookcountyil.gov>, Robert Lunk (Sheriff) <Robert.Lunk@cookcountyil.gov>

Sent: June 30, 2020 8:06:39 AM CDT

Received: June 30, 2020 8:06:41 AM CDT

Attachments: (U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

Please see the attached DHS Intelligence Brief, “Criminal Hackers Target US Law Enforcement Data,” dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

If you no longer wish to be on this distribution list, please send an email to ccso.intel@cookcountyil.gov to discontinue receiving these emails. If you would like any member under your command to receive these emails, please send an email to ccso.intel@cookcountyil.gov and include their name, title and email address in the body of the request.

Cook County Sheriff's Office
Strategic Operations Center
3026 S. California Avenue
Building 5, 2nd Floor
Chicago, IL. 60608
Office: 773-674-2694 or 8477
Fax: 773-674-4797

THIS IS A CONFIDENTIAL LAW ENFORCEMENT COMMUNICATION. The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential. If you are not the intended recipient of this message, or if this message has been addressed to you in error, please immediately alert the sender by reply e-mail and then delete this message and its attachments. Do not deliver, distribute, transmit or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action relative to the information contained in this communication and/or attachments. This e-mail and any attached documents may contain For Official Use Only and/or Law Enforcement Sensitive material and should not be disseminated outside of official law enforcement channels. The information contained in this message as well as any attachments shall not be released to the media or the general public.

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

Sent: June 30, 2020 8:07:20 AM CDT
Received: June 30, 2020 8:07:29 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Sheriff Intel
Sent:	June 30, 2020 8:07:20 AM CDT
Received:	June 30, 2020 8:07:26 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Adam Murphy (Sheriff)
Sent:	June 30, 2020 8:07:20 AM CDT
Received:	June 30, 2020 8:07:26 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Juan Claudio (Sheriff)
Sent: June 30, 2020 8:07:20 AM CDT
Received: June 30, 2020 8:07:26 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Andre Blue (Sheriff)
Sent:	June 30, 2020 8:07:20 AM CDT
Received:	June 30, 2020 8:07:29 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Joseph Scofield (Sheriff)
Sent: June 30, 2020 8:07:20 AM CDT
Received: June 30, 2020 8:07:26 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Jaunesh Contreras (Sheriff)
Sent: June 30, 2020 8:07:20 AM CDT
Received: June 30, 2020 8:07:29 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Joseph Nicholas (Sheriff)
Sent: June 30, 2020 8:07:20 AM CDT
Received: June 30, 2020 8:07:27 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Antoinette Bradley (Sheriff)
Sent:	June 30, 2020 8:07:20 AM CDT
Received:	June 30, 2020 8:07:27 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Arthur Jackson (Sheriff)
Sent:	June 30, 2020 8:07:20 AM CDT
Received:	June 30, 2020 8:07:26 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	David Cammack (Sheriff)
Sent:	June 30, 2020 8:07:20 AM CDT
Received:	June 30, 2020 8:07:27 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Jasmina Janjic (Sheriff)
Sent:	June 30, 2020 8:07:20 AM CDT
Received:	June 30, 2020 8:07:26 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Joseph Rosenau (Sheriff)
Sent: June 30, 2020 8:07:20 AM CDT
Received: June 30, 2020 8:07:26 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Gustavo Jimenez (Sheriff)
Sent:	June 30, 2020 8:07:20 AM CDT
Received:	June 30, 2020 8:07:28 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	John Konrad (Sheriff)
Sent:	June 30, 2020 8:07:20 AM CDT
Received:	June 30, 2020 8:07:29 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Adrian Molina (Sheriff)
Sent:	June 30, 2020 8:07:20 AM CDT
Received:	June 30, 2020 8:07:26 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Kevin O'Donnell (Sheriff)
Sent: June 30, 2020 8:07:20 AM CDT
Received: June 30, 2020 8:07:26 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Christopher Harvey (Sheriff)
Sent:	June 30, 2020 8:07:20 AM CDT
Received:	June 30, 2020 8:07:26 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Jerome Ryan (Sheriff)
Sent: June 30, 2020 8:07:20 AM CDT
Received: June 30, 2020 8:07:26 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Brian Staudt (Sheriff)
Sent:	June 30, 2020 8:07:20 AM CDT
Received:	June 30, 2020 8:07:26 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Joseph Phillips (Sheriff)
Sent: June 30, 2020 8:07:20 AM CDT
Received: June 30, 2020 8:07:27 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Fulvio Compagnone (Sheriff)
Sent:	June 30, 2020 8:07:20 AM CDT
Received:	June 30, 2020 8:07:26 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From: CCSO Intel (Sheriff) <CCSO.INTEL@cookcountyil.gov>

Bcc: Aaron Cadena (Sheriff) <Aaron.Cadena@cookcountyil.gov>, Aaron Spears (Sheriff) <Aaron.Spears@cookcountyil.gov>, Abel Torres (Sheriff) <Abel.Torres@cookcountyil.gov>, Abelardo Mercado (Sheriff) <Abelardo.Mercado@cookcountyil.gov>, Adam Dowdell (Sheriff) <Adam.Dowdell@cookcountyil.gov>, Adam Lachecki (Sheriff) <Adam.Lachecki@cookcountyil.gov>, Adam Lemons (Sheriff) <Adam.Lemons@cookcountyil.gov>, Adam Murphy (Sheriff) <Adam.Murphy@cookcountyil.gov>, Adam Stafiera (Sheriff) <Adam.Stafiera@cookcountyil.gov>, Adrian Cerchez (Sheriff) <Adrian.Cerchez@cookcountyil.gov>, Adrian Molina (Sheriff) <Adrian.Molina@cookcountyil.gov>, Adrian Sandoval (Sheriff) <Adrian.Sandoval@cookcountyil.gov>, Aisha Wade (Sheriff) <Aisha.Wade@cookcountyil.gov>, Alan Kickert (Sheriff) <Alan.Kickert@cookcountyil.gov>, Aleshia Maurer (Sheriff) <Aleshia.Maurer@cookcountyil.gov>, Alexander Brodie (Sheriff) <Alexander.Brodie@cookcountyil.gov>, Alexandra Bouziotis (Sheriff) <Alexandra.Bouziotis@cookcountyil.gov>, Alfredo Garcia (Sheriff) <Alfredo.Garcia@cookcountyil.gov>, Allen Giacchetti (Sheriff) <Allen.Giacchetti@cookcountyil.gov>, Alvin Coleman (Sheriff) <Alvin.Coleman@cookcountyil.gov>, Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Ambrose Kelly (Sheriff) <Ambrose.Kelly@cookcountyil.gov>, Amy Lilliebridge (Sheriff) <Amy.Lilliebridge@cookcountyil.gov>, Ana Rivera (Sheriff) <Ana.Rivera@cookcountyil.gov>, Andre Blue (Sheriff) <Andre.Blue@cookcountyil.gov>, Andrew Douvris (Sheriff) <Andrew.Douvris@cookcountyil.gov>, Andrew Gutter (Sheriff) <Andrew.Gutter@cookcountyil.gov>, Andrew Tucker (Sheriff) <Andrew.Tucker@cookcountyil.gov>, Angel Garcia (Sheriff) <Angel.Garcia2@cookcountyil.gov>, Angela Thornton (Sheriff) <Angela.Thornton@cookcountyil.gov>, Anita Dix-Lindsey (Sheriff) <Anita.Dix-Lindsey@cookcountyil.gov>, Anna Wilk (Sheriff) <Anna.Wilk@cookcountyil.gov>, Anthony Aguirre (Sheriff) <Anthony.Aguirre@cookcountyil.gov>, Anthony Burns (Sheriff) <Anthony.Burns@cookcountyil.gov>, Anthony Cortesi (Sheriff) <Anthony.Cortesi@cookcountyil.gov>, Anthony Kozlar (Sheriff) <Anthony.Kozlar@cookcountyil.gov>, Anthony Licata (Sheriff) <Anthony.Licata2@cookcountyil.gov>, Anthony Ochoa (Sheriff) <Anthony.Ochoa@cookcountyil.gov>, Anthony Roche (Sheriff) <Anthony.Roche@cookcountyil.gov>, Anthony Schickel (Sheriff) <Anthony.Schickel@cookcountyil.gov>, Anthony Stack (Sheriff) <Anthony.Stack@cookcountyil.gov>, Antoinette Bradley (Sheriff) <Antoinette.Bradley@cookcountyil.gov>, Antwann Boyd (Sheriff) <Antwann.Boyd@cookcountyil.gov>, Armando Gutierrez (Sheriff) <Armando.Gutierrez2@cookcountyil.gov>, Armando Gutierrez (Sheriff) <Armando.Gutierrez@cookcountyil.gov>, Arthur Jackson (Sheriff) <Arthur.Jackson@cookcountyil.gov>, Arthur Taylor (Sheriff) <Arthur.Taylor@cookcountyil.gov>, Augie Fabela (Sheriff) <Augie.Fabela@cookcountyil.gov>, Barbara Dymitrowicz (Sheriff) <Barbara.Dymitrowicz@cookcountyil.gov>, Barbara Perduto (Sheriff) <Barbara.Perduto@cookcountyil.gov>, Beatrice Winfert-Quan (Sheriff) <Beatrice.Winfert-Quan@cookcountyil.gov>, Beatriz Vigil (Sheriff) <Beatriz.Vigil3@cookcountyil.gov>, Benjamin Sullivan (Sheriff) <Benjamin.Sullivan@cookcountyil.gov>, Benjamin VonOhlen (Sheriff) <Benjamin.Vonohlen@cookcountyil.gov>, Beverly Austin (Sheriff) <Beverly.Austin@cookcountyil.gov>, Bonnie Busching (Sheriff) <Bonnie.Busching@cookcountyil.gov>, Brandon Ducray (Sheriff) <Brandon.Ducray@cookcountyil.gov>, Brenda McKendrick (Sheriff) <Brenda.Mckendrick@cookcountyil.gov>, Brendan Behan (Sheriff) <Brendan.Behan@cookcountyil.gov>, Brian Abels (Sheriff)

<Brian.Abels@cookcountyil.gov>, Brian Atkinson (Sheriff)
<Brian.Atkinson@cookcountyil.gov>, Brian Bonarek (Sheriff)
<Brian.Bonarek@cookcountyil.gov>, Brian Dignan (Sheriff)
<Brian.Dignan@cookcountyil.gov>, Brian Hartsfield (Sheriff)
<Brian.Hartsfield@cookcountyil.gov>, Brian Helstern (Sheriff)
<Brian.Helstern@cookcountyil.gov>, Brian Manthey (Sheriff)
<Brian.Manthey@cookcountyil.gov>, Brian Matos (Sheriff)
<Brian.Matos@cookcountyil.gov>, Brian McNamara (Sheriff)
<Brian.Mcnamara@cookcountyil.gov>, Brian Staudt (Sheriff)
<Brian.Staudt@cookcountyil.gov>, Brian Toner (Sheriff)
<Brian.Toner@cookcountyil.gov>, Brian Toosley (Sheriff)
<Brian.Toosley@cookcountyil.gov>, Brian White (Sheriff)
<Brian.White@cookcountyil.gov>, Brittney Blair (Sheriff)
<Brittney.Blair@cookcountyil.gov>, Bruce Steinke (Sheriff)
<Bruce.Steinke@cookcountyil.gov>, Bryant Walker (Sheriff)
<Bryant.Walker@cookcountyil.gov>, Cameron Pon (Sheriff)
<Cameron.Pon@cookcountyil.gov>, Carl Campbell (Sheriff)
<Carl.Campbell@cookcountyil.gov>, Carl Oviedo (Sheriff)
<Carl.Oviedo@cookcountyil.gov>, Carl Shaw (Sheriff)
<Carl.Shaw@cookcountyil.gov>, Carlos Martinez (Sheriff)
<Carlos.Martinez@cookcountyil.gov>, Carmelo Reillo (Sheriff)
<Carmelo.Reillo@cookcountyil.gov>, Cassy Poirier (Sheriff)
<Cassy.Poirier@cookcountyil.gov>, Catherine Belluomini (Sheriff)
<Catherine.Belluomini@cookcountyil.gov>, Catherine DiGiovanni (Sheriff)
<Catherine.DiGiovanni@cookcountyil.gov>, Catherine Domine (Sheriff)
<Catherine.Domine@cookcountyil.gov>, Catherine Fitzgerald (Sheriff)
<Catherine.Fitzgerald@cookcountyil.gov>, Catherine Mellett (Sheriff)
<Catherine.Mellett@cookcountyil.gov>, Cathy Ryan (Sheriff)
<Cathy.Ryan@cookcountyil.gov>, Cedric Brantley (Sheriff)
<Cedric.Brantley@cookcountyil.gov>, Cedric Mc Cloud (Sheriff)
<Cedric.Mccloud@cookcountyil.gov>, Cesar Carbajal (Sheriff)
<Cesar.Carbajal@cookcountyil.gov>, Chad Bonen (Sheriff)
<Chad.Bonen@cookcountyil.gov>, Charles Graf (Sheriff)
<Charles.Graf@cookcountyil.gov>, Charles Henderson (Sheriff)
<Charles.Henderson@cookcountyil.gov>, Charles Little (Sheriff)
<Charles.Little@cookcountyil.gov>, Charles Olson (Sheriff)
<Charles.Olson@cookcountyil.gov>, Christie Urso (Sheriff)
<Christie.Urso@cookcountyil.gov>, Christina Nedved (Sheriff)
<Christina.Nedved@cookcountyil.gov>, Christine Bertucci (Sheriff)
<Christine.Bertucci@cookcountyil.gov>, Christine Gallagher (Sheriff)
<Christine.Gallagher@cookcountyil.gov>, Christine Miller (Sheriff)
<Christine.Miller@cookcountyil.gov>, Christopher Arocho (Sheriff)
<Christopher.Arocho@cookcountyil.gov>, Christopher Boyle (Sheriff)
<Christopher.Boyle@cookcountyil.gov>, Christopher Calhoun (Sheriff)
<Christopher.Calhoun@cookcountyil.gov>, Christopher Dangles (Sheriff)
<Christopher.Dangles@cookcountyil.gov>, Christopher Garcia (Sheriff)
<Christopher.Garcia1@cookcountyil.gov>, Christopher Harris (Sheriff)
<Christopher.Harris@cookcountyil.gov>, Christopher Harvey (Sheriff)
<Christopher.Harvey@cookcountyil.gov>, Christopher Imhof (Sheriff)
<Christopher.Imhof@cookcountyil.gov>, Christopher Lanuti (Sheriff)
<Christopher.Lanuti@cookcountyil.gov>, Christopher McDonough (Sheriff)
<Christopher.Mcdonough@cookcountyil.gov>, Christopher Olejarz (Sheriff)
<Christopher.Olejarz@cookcountyil.gov>, Christopher Rago (Sheriff)
<Christopher.Rago@cookcountyil.gov>, Christopher Suggs (Sheriff)
<Christopher.Suggs@cookcountyil.gov>, Cierra Thurman (Sheriff)
<Cierra.Thurman@cookcountyil.gov>, Cody Lettiere (Sheriff)
<Cody.Lettiere@cookcountyil.gov>, Conley Dyer (Sheriff)
<Conley.Dyer@cookcountyil.gov>, Conrad Edgett (Sheriff)
<Conrad.Edgett@cookcountyil.gov>, Corey Russell (Sheriff)
<Corey.Russell@cookcountyil.gov>, Craig Wilk (Sheriff)
<Craig.Wilk@cookcountyil.gov>, Dan Nowotarski (Sheriff)
<Dan.Nowotarski@cookcountyil.gov>, Daniel Alvarado (Sheriff)
<Daniel.Alvarado@cookcountyil.gov>, Daniel Borosz (Sheriff)

<Daniel.Borosz@cookcountyil.gov>, Daniel Burke (Sheriff)
<Daniel.Burke@cookcountyil.gov>, Daniel Codd (Sheriff)
<Daniel.Codd@cookcountyil.gov>, Daniel Dehoyos (Sheriff)
<Daniel.DeHoyos@cookcountyil.gov>, Daniel Gmiterek (Sheriff)
<Daniel.Gmiterek@cookcountyil.gov>, Daniel Keserich (Sheriff)
<Daniel.Keserich@cookcountyil.gov>, Daniel Lopez (Sheriff)
<Daniel.Lopez@cookcountyil.gov>, Daniel Mo (Sheriff)
<Daniel.Mo@cookcountyil.gov>, Daniel Pollard (Sheriff)
<Daniel.Pollard@cookcountyil.gov>, Daniel Redican (Sheriff)
<Daniel.Redican@cookcountyil.gov>, Daniel Schaller (Sheriff)
<Daniel.Schaller@cookcountyil.gov>, Daniel Strong (Sheriff)
<Daniel.Strong@cookcountyil.gov>, Daniel Woods (Sheriff)
<Daniel.Woods@cookcountyil.gov>, Darryl Anthony (Sheriff)
<Darryl.Anthony@cookcountyil.gov>, Darryl Ashley (Sheriff)
<Darryl.Ashley@cookcountyil.gov>, Darryl Manning (Sheriff)
<Darryl.Manning@cookcountyil.gov>, Daryl Demro (Sheriff)
<Daryl.Demro@cookcountyil.gov>, Dave Hardy (Sheriff)
<Dave.Hardy@cookcountyil.gov>, David Baez (Sheriff)
<David.Baez@cookcountyil.gov>, David Bily (Sheriff)
<David.Bily@cookcountyil.gov>, David Buffham (Sheriff)
<David.Buffham@cookcountyil.gov>, David Cammack (Sheriff)
<David.Cammack@cookcountyil.gov>, David Carroll (Sheriff)
<David.Carroll@cookcountyil.gov>, David Delgado (Sheriff)
<David.Delgado1@cookcountyil.gov>, David Krok (Sheriff)
<David.Krok@cookcountyil.gov>, David Lomax (Sheriff)
<David.Lomax@cookcountyil.gov>, David Ribaldo (Sheriff)
<David.Ribaldo@cookcountyil.gov>, David Sokolowski (Sheriff)
<David.Sokolowski@cookcountyil.gov>, David Stanly (Sheriff)
<David.Stanly@cookcountyil.gov>, David Stiak (Sheriff)
<David.Stiak@cookcountyil.gov>, David Tuzim (Sheriff)
<David.Tuzim@cookcountyil.gov>, David Witkowski (Sheriff)
<David.Witkowski@cookcountyil.gov>, Dedra Cummins (Sheriff)
<Dedra.Cummins@cookcountyil.gov>, Delisa Spears (Sheriff)
<Delisa.Spears@cookcountyil.gov>, Demetrius Nichols (Sheriff)
<Demetrius.Nichols@cookcountyil.gov>, Denise Banda (Sheriff)
<Denise.Banda@cookcountyil.gov>, Denise Demichel (Sheriff)
<Denise.Demichel@cookcountyil.gov>, Deon Tate (Sheriff)
<Deon.Tate@cookcountyil.gov>, Derek Fabian (Sheriff)
<Derek.Fabian@cookcountyil.gov>, Derrick Trice (Sheriff)
<Derrick.Trice@cookcountyil.gov>, Devlin Gray (Sheriff)
<Devlin.Gray@cookcountyil.gov>, Diane Haras (Sheriff)
<Diane.Haras@cookcountyil.gov>, Dimas Hernandez (Sheriff)
<Dimas.Hernandez@cookcountyil.gov>, Dion Trotter (Sheriff)
<Dion.Trotter@cookcountyil.gov>, Dominic Boggia (Sheriff)
<Dominic.Boggia@cookcountyil.gov>, Dominique Deal (Sheriff)
<Dominique.Deal@cookcountyil.gov>, Don Stewart (Sheriff)
<Don.Stewart@cookcountyil.gov>, Donald Buczkowski (Sheriff)
<Donald.Buczkowski@cookcountyil.gov>, Donald Harris (Sheriff)
<Donald.Harris@cookcountyil.gov>, Dorian Swain (Sheriff)
<Dorian.Swain@cookcountyil.gov>, Douglas Crawford (Sheriff)
<Douglas.Crawford@cookcountyil.gov>, Douglas Schultz (Sheriff)
<Douglas.Schultz@cookcountyil.gov>, Eddie Ishoo (Sheriff)
<Eddie.Ishoo@cookcountyil.gov>, Edmundo Hernandez (Sheriff)
<Edmundo.Hernandez@cookcountyil.gov>, Eduardo Hower (Sheriff)
<Eduardo.Hower@cookcountyil.gov>, Edward Barksdale (Sheriff)
<Edward.Barksdale@cookcountyil.gov>, Edward Graney (Sheriff)
<Edward.Graney@cookcountyil.gov>, Edward Lewandowski (Sheriff)
<Edward.Lewandowski@cookcountyil.gov>, Eevandia Weatherly (Sheriff)
<Eevandia.Weatherly@cookcountyil.gov>, Efrain Mata (Sheriff)
<Efrain.Mata@cookcountyil.gov>, Eliezer Pacheco (Sheriff)
<Eliezer.Pacheco@cookcountyil.gov>, Elizabeth Collins (Sheriff)
<Elizabeth.Collins@cookcountyil.gov>, Elizabeth McCarthy (Sheriff)
<Elizabeth.McCarthy@cookcountyil.gov>, Elliott Feliciano (Sheriff)

<Elliott.Feliciano@cookcountyil.gov>, Elliott Reyes (Sheriff)
<Elliott.Reyes@cookcountyil.gov>, Enrique Nieves (Sheriff)
<Enrique.Nieves@cookcountyil.gov>, Enver Vejzovic (Sheriff)
<Enver.Vejzovic@cookcountyil.gov>, Eric Burnson (Sheriff)
<Eric.Burnson@cookcountyil.gov>, Eric Maurer (Sheriff)
<Eric.Maurer@cookcountyil.gov>, Eric Przybycien (Sheriff)
<Eric.Przybycien@cookcountyil.gov>, Eric Sellers (Sheriff)
<Eric.Sellers@cookcountyil.gov>, Eric Siciliano (Sheriff)
<Eric.Siciliano@cookcountyil.gov>, Erik Roedel (Sheriff)
<Erik.Roedel@cookcountyil.gov>, Erika Rodriguez (Sheriff)
<Erika.Rodriguez2@cookcountyil.gov>, Erin Hamilton (Sheriff)
<Erin.Hamilton@cookcountyil.gov>, Eryn T Hedderman (Sheriff)
<Eryn.Hedderman@cookcountyil.gov>, Eugene Butler (Sheriff)
<Eugene.Butler@cookcountyil.gov>, Eyad Awad (Sheriff)
<Eyad.Awad@cookcountyil.gov>, Faliata Holman (Sheriff)
<Faliata.Holman@cookcountyil.gov>, Faviana Leon (Sheriff)
<Faviana.Leon@cookcountyil.gov>, Felix Arvelo (Sheriff)
<Felix.Arvelo@cookcountyil.gov>, Foster Bradley (Sheriff)
<Foster.Bradley@cookcountyil.gov>, Francisco Ruiz (Sheriff)
<Francisco.Ruiz@cookcountyil.gov>, Frank Caridei (Sheriff)
<Frank.Caridei@cookcountyil.gov>, Frank D'oronzo (Sheriff)
<Frank.Doronzo@cookcountyil.gov>, Frank Medrys (Sheriff)
<Frank.Medrys@cookcountyil.gov>, Frank Washington (Sheriff)
<Frank.Washington@cookcountyil.gov>, Frank Wisniewski (Sheriff)
<Frank.Wisniewski@cookcountyil.gov>, Frederick Nowaczyk (Sheriff)
<Frederick.Nowaczyk@cookcountyil.gov>, Froylan Mena (Sheriff)
<Froylan.Mena@cookcountyil.gov>, Fulvio Compagnone (Sheriff)
<Fulvio.Compagnone@cookcountyil.gov>, Gary Contreras (Sheriff)
<Gary.Contreras@cookcountyil.gov>, Gary Newsom (Sheriff)
<Gary.Newsom@cookcountyil.gov>, Gary Rizzo (Sheriff)
<Gary.Rizzo@cookcountyil.gov>, Genevieve Voves (Sheriff)
<Genevieve.Voves@cookcountyil.gov>, George Anton (Sheriff)
<George.Anton@cookcountyil.gov>, George Marks (Sheriff)
<George.Marks@cookcountyil.gov>, George Velisaris (Sheriff)
<George.Velisaris@cookcountyil.gov>, Gerald Chickerillo (Sheriff)
<Gerald.Chickerillo@cookcountyil.gov>, Gilberto Romero (Sheriff)
<Gilberto.Romero@cookcountyil.gov>, Ginny Georgantas (Sheriff)
<Ginny.Georgantas@cookcountyil.gov>, Giovanni.Veitkus@cookcountyil.gov, Gordon Brewer (Sheriff) <Gordon.Brewer@cookcountyil.gov>, Grazyna Moczarna (Sheriff) <Grazyna.Moczarna@cookcountyil.gov>, Gregory Barron (Sheriff) <Gregory.Barron@cookcountyil.gov>, Gregory Kulasa (Sheriff)
<Gregory.Kulasa@cookcountyil.gov>, Gregory Sandquist (Sheriff)
<Gregory.Sandquist@cookcountyil.gov>, Gregory Vlahos (Sheriff)
<Gregory.Vlahos@cookcountyil.gov>, Gustavo Jimenez (Sheriff)
<Gustavo.Jimenez@cookcountyil.gov>, Harry Vance (Sheriff)
<Harry.Vance@cookcountyil.gov>, Heather Bock (Sheriff)
<Heather.Bock@cookcountyil.gov>, Heather Jaycox (Sheriff)
<Heather.Jaycox@cookcountyil.gov>, Hector Mendez (Sheriff)
<Hector.Mendez@cookcountyil.gov>, Helen O'Connor (Sheriff)
<Helen.O'connor@cookcountyil.gov>, Helen Siaj (Sheriff)
<Helen.Siaj@cookcountyil.gov>, Henry Macugowski (Sheriff)
<Henry.Macugowski@cookcountyil.gov>, Henry Rush (Sheriff)
<Henry.Rush@cookcountyil.gov>, Henry Washington (Sheriff)
<Henry.Washington@cookcountyil.gov>, Irene Salinas (Sheriff)
<Irene.Salinas@cookcountyil.gov>, Iseano McDonald (Sheriff)
<Iseano.Mcdonald@cookcountyil.gov>, Issac Thomas (Sheriff)
<Issac.Thomas@cookcountyil.gov>, Ivan Salva (Sheriff)
<Ivan.Salva@cookcountyil.gov>, Jacob Moran (Sheriff)
<Jacob.Moran@cookcountyil.gov>, Jacqueline Brown (Sheriff)
<Jacqueline.Brown2@cookcountyil.gov>, Jacqueline Lazzara (Sheriff)
<Jacqueline.Lazzara@cookcountyil.gov>, Jae Bae (Sheriff)
<Jae.Bae@cookcountyil.gov>, Jae Bae1 (Sheriff)
<Jae.Bae2@cookcountyil.gov>, Jaime Martinez (Sheriff)

<Jaime.Martinez2@cookcountyil.gov>, Jaime Martinez (Sheriff)
<Jaime.Martinez3@cookcountyil.gov>, James Anichini (Sheriff)
<James.Anichini@cookcountyil.gov>, James Bolek (Sheriff)
<James.Bolek@cookcountyil.gov>, James Davis (Sheriff)
<James.Davis@cookcountyil.gov>, James Draz (Sheriff)
<James.Draz@cookcountyil.gov>, James Goodman (Sheriff)
<James.Goodman@cookcountyil.gov>, James Gosling (Sheriff)
<James.Gosling@cookcountyil.gov>, James Harris (Sheriff)
<James.Harris@cookcountyil.gov>, James Hughes (Sheriff)
<James.Hughes@cookcountyil.gov>, James Mc Caffrey (Sheriff)
<James.Mccaffrey@cookcountyil.gov>, James Pacetti (Sheriff)
<James.Pacetti@cookcountyil.gov>, James Plybon (Sheriff)
<James.Plybon@cookcountyil.gov>, James Scannell (Sheriff)
<James.Scannell@cookcountyil.gov>, James Torelli (Sheriff)
<James.Torelli@cookcountyil.gov>, Jami Koprowski (Sheriff)
<Jami.Koprowski@cookcountyil.gov>, Jarius Dixon (Sheriff)
<Jarius.Dixon@cookcountyil.gov>, Jaron Lee (Sheriff)
<Jaron.Lee@cookcountyil.gov>, Jasmina Janjic (Sheriff)
<Jasmina.Janjic@cookcountyil.gov>, Jason Broadway (Sheriff)
<Jason.Broadway@cookcountyil.gov>, Jason Doeslaere (Sheriff)
<Jason.Doeslaere@cookcountyil.gov>, Jason Moran (Sheriff)
<Jason.Moran@cookcountyil.gov>, Jason O'Malley (Sheriff)
<Jason.O'Malley@cookcountyil.gov>, Jason Schmidt (Sheriff)
<Jason.Schmidt@cookcountyil.gov>, Jasper Nelson (Sheriff)
<Jasper.Nelson@cookcountyil.gov>, Jaunesh Contreras (Sheriff)
<Jaunesh.Contreras@cookcountyil.gov>, Javier Alvarez (Sheriff)
<Javier.Alvarez@cookcountyil.gov>, Jeff Guay (Sheriff)
<Jeff.Guay@cookcountyil.gov>, Jeffrey Ansted (Sheriff)
<Jeffrey.Ansted@cookcountyil.gov>, Jeffrey Ramos (Sheriff)
<Jeffrey.Ramos@cookcountyil.gov>, Jeffrey Trost (Sheriff)
<Jeffrey.Trost@cookcountyil.gov>, Jeffrey.Pasqua@cookcountyil.gov,
Jennifer Nowaczyk (Sheriff) <Jennifer.Nowaczyk@cookcountyil.gov>, Jerome
Ryan (Sheriff) <Jerome.Ryan@cookcountyil.gov>, Jershawn Dubose (Sheriff)
<Jershawn.Dubose@cookcountyil.gov>, Jessica Gatti (Sheriff)
<Jessica.Gatti@cookcountyil.gov>, Jessica McCants (Sheriff)
<Jessica.McCants@cookcountyil.gov>, Jessica Thomas (Sheriff)
<Jessica.Thomas@cookcountyil.gov>, Jimeal Haddad (Sheriff)
<Jimeal.Haddad@cookcountyil.gov>, Jimmy Olle (Sheriff)
<Jimmy.Olle@cookcountyil.gov>, Joanna Ryan (Sheriff)
<Joanna.Ryan@cookcountyil.gov>, Joe Dugandzic (Sheriff)
<Joe.Dugandzic@cookcountyil.gov>, John Aguilera (Sheriff)
<John.Aguilera2@cookcountyil.gov>, John Barloga (Sheriff)
<John.Barloga@cookcountyil.gov>, John Bennett (Sheriff)
<John.Bennett@cookcountyil.gov>, John Blair (Sheriff)
<John.Blair@cookcountyil.gov>, John Braun (Sheriff)
<John.Braun@cookcountyil.gov>, John Dziedzic (Sheriff)
<John.Dziedzic@cookcountyil.gov>, John Files (Sheriff)
<John.Files@cookcountyil.gov>, John Gallagher (Sheriff)
<John.Gallagher@cookcountyil.gov>, John Konrad (Sheriff)
<John.Konrad@cookcountyil.gov>, John Kowalczyk (Sheriff)
<John.Kowalczyk@cookcountyil.gov>, John Kruswicki (Sheriff)
<John.Kruswicki@cookcountyil.gov>, John Merola (Sheriff)
<John.Merola@cookcountyil.gov>, John Nawara (Sheriff)
<John.Nawara@cookcountyil.gov>, John O'Farrell (Sheriff)
<John.Ofarrell@cookcountyil.gov>, John Pradun (Sheriff)
<John.Pradun@cookcountyil.gov>, John Riggio (Sheriff)
<John.Riggio@cookcountyil.gov>, John Simone (Sheriff)
<John.Simone@cookcountyil.gov>, John Slepski (Sheriff)
<John.Slepski@cookcountyil.gov>, John Steed (Sheriff)
<John.Steed@cookcountyil.gov>, John Sullivan (Sheriff)
<John.Sullivan2@cookcountyil.gov>, John Vega (Sheriff)
<John.Vega@cookcountyil.gov>, Johnny Cantu (Sheriff)
<Johnny.Cantu@cookcountyil.gov>, Jonathan Janulis (Sheriff)

<Jonathan.Janulis@cookcountyil.gov>, Jonathan Pilli (Sheriff)
<Jonathan.Pilli@cookcountyil.gov>, Jonathan.Mobley@cookcountyil.gov,
Jordan Green (Sheriff) <Jordan.Green@cookcountyil.gov>, Jorge Gali (Sheriff)
<Jorge.Gali@cookcountyil.gov>, Jorge Mayen (Sheriff)
<Jorge.Mayen@cookcountyil.gov>, Jose Delvalle (Sheriff)
<Jose.Delvalle@cookcountyil.gov>, Jose Madrid (Sheriff)
<Jose.Madrid@cookcountyil.gov>, Jose Martinez (Sheriff)
<Jose.Martinez2@cookcountyil.gov>, Jose Reyna (Sheriff)
<Jose.Reyna@cookcountyil.gov>, Jose Rodriguez (Sheriff)
<Jose.Rodriguez4@cookcountyil.gov>, Jose Rosario (Sheriff)
<Jose.Rosario@cookcountyil.gov>, Joseph Alva (Sheriff)
<Joseph.Alva@cookcountyil.gov>, Joseph Burdi (Sheriff)
<Joseph.Burdi@cookcountyil.gov>, Joseph Calderone (Sheriff)
<Joseph.Calderone@cookcountyil.gov>, Joseph Chirillo (Sheriff)
<Joseph.Chirillo@cookcountyil.gov>, Joseph Dale (Sheriff)
<Joseph.Dale@cookcountyil.gov>, Joseph Gudella (Sheriff)
<Joseph.Gudella@cookcountyil.gov>, Joseph Maselko (Sheriff)
<Joseph.Maselko@cookcountyil.gov>, Joseph McGough (Sheriff)
<Joseph.McGough@cookcountyil.gov>, Joseph Nicholas (Sheriff)
<Joseph.Nicholas@cookcountyil.gov>, Joseph Park (Sheriff)
<Joseph.Park@cookcountyil.gov>, Joseph Phillips (Sheriff)
<Joseph.Phillips@cookcountyil.gov>, Joseph Piersanti (Sheriff)
<Joseph.Piersanti@cookcountyil.gov>, Joseph Rosenau (Sheriff)
<Joseph.Rosenau@cookcountyil.gov>, Joseph Scofield (Sheriff)
<Joseph.Scofield@cookcountyil.gov>, Joseph Smith (Sheriff)
<Joseph.Smith@cookcountyil.gov>, Joseph Vertucci (Sheriff)
<Joseph.Vertucci@cookcountyil.gov>, Joshua Johnson (Sheriff)
<Joshua.Johnson@cookcountyil.gov>, Joyce Lowery (Sheriff)
<Joyce.Lowery@cookcountyil.gov>, Juan Arellano (Sheriff)
<Juan.Arellano@cookcountyil.gov>, Juan Claudio (Sheriff)
<Juan.Claudio@cookcountyil.gov>, Juan Irizarry (Sheriff)
<Juan.Irizarry@cookcountyil.gov>, Juan Mata (Sheriff)
<Juan.Mata@cookcountyil.gov>, Juan Tapia (Sheriff)
<Juan.Tapia@cookcountyil.gov>, Juan Velez (Sheriff)
<Juan.Velez@cookcountyil.gov>, Juanita Blaino (Sheriff)
<Juanita.Blaino@cookcountyil.gov>, Judith Powe (Sheriff)
<Judith.Powe@cookcountyil.gov>, Julie Duffy (Sheriff)
<Julie.Duffy@cookcountyil.gov>, Julie Spencer (Sheriff)
<Julie.Spencer@cookcountyil.gov>, Justin Jones (Sheriff)
<Justin.Jones@cookcountyil.gov>, Kanisha Rodriguez (Sheriff)
<Kanisha.Rodriguez@cookcountyil.gov>, Karen Amegatcher (Sheriff)
<Karen.Amegatcher@cookcountyil.gov>, Karl Thomas (Sheriff)
<Karl.Thomas@cookcountyil.gov>, Karol Suchocki (Sheriff)
<Karol.Suchocki@cookcountyil.gov>, Katarzyna Wells (Sheriff)
<Katarzyna.Wells@cookcountyil.gov>, Katherine Walsh (Sheriff)
<Katherine.Walsh@cookcountyil.gov>, Kathleen Efta (Sheriff)
<Kathleen.Efta@cookcountyil.gov>, Keena Bradley (Sheriff)
<Keena.Bradley@cookcountyil.gov>, Keith Garner (Sheriff)
<Keith.Garner@cookcountyil.gov>, Keith Gray (Sheriff)
<Keith.Gray@cookcountyil.gov>, Keith Mc Carter (Sheriff)
<Keith.McCarter@cookcountyil.gov>, Keith Morrison (Sheriff)
<Keith.Morrison@cookcountyil.gov>, Kelley Kleist (Sheriff)
<Kelley.Kleist@cookcountyil.gov>, Kelly Rohe (Sheriff)
<Kelly.Rohe2@cookcountyil.gov>, Kelly Stott (Sheriff)
<Kelly.Stott@cookcountyil.gov>, Kelly Sweeney (Sheriff)
<Kelly.Sweeney@cookcountyil.gov>, Kelvin Blanchard (Sheriff)
<Kelvin.Blanchard@cookcountyil.gov>, Kendall Evans (Sheriff)
<Kendall.Evans@cookcountyil.gov>, Kenneth Vargas (Sheriff)
<Kenneth.Vargas@cookcountyil.gov>, Keri Baker (Sheriff)
<Keri.Baker@cookcountyil.gov>, Kevin Badon (Sheriff)
<Kevin.Badon@cookcountyil.gov>, Kevin Boens (Sheriff)
<Kevin.Boens@cookcountyil.gov>, Kevin Christofidis (Sheriff)
<Kevin.Christofidis@cookcountyil.gov>, Kevin Cooper (Sheriff)

<Kevin.Cooper@cookcountyil.gov>, Kevin Ellis (Sheriff)
<Kevin.Ellis@cookcountyil.gov>, Kevin Enyart (Sheriff)
<Kevin.Enyart@cookcountyil.gov>, Kevin Farrell (Sheriff)
<Kevin.Farrell@cookcountyil.gov>, Kevin Graff (Sheriff)
<Kevin.Graff@cookcountyil.gov>, Kevin Kelly (Sheriff)
<Kevin.Kelly@cookcountyil.gov>, Kevin O'Donnell (Sheriff)
<Kevin.Odonnell@cookcountyil.gov>, Kevin O'Reilly (Sheriff)
<Kevin.Oreilly@cookcountyil.gov>, Kevin Ruel (Sheriff)
<Kevin.Ruel@cookcountyil.gov>, Kevin Suchocki (Sheriff)
<Kevin.Suchocki@cookcountyil.gov>, Kevin Tomkins (Sheriff)
<Kevin.Tomkins@cookcountyil.gov>, Kevin Walsh (Sheriff)
<Kevin.Walsh@cookcountyil.gov>, Khaleelah Sneed (Sheriff)
<Khaleelah.Sneed@cookcountyil.gov>, Kiersten Kendall (Sheriff)
<Kiersten.Kendall@cookcountyil.gov>, Kimberley Guerin (Sheriff)
<Kimberley.Guerin@cookcountyil.gov>, Kimberly Brown (Sheriff)
<Kimberly.Brown@cookcountyil.gov>, Kimberly Capelli (Sheriff)
<Kimberly.Capelli@cookcountyil.gov>, Kimberly Germain (Sheriff)
<Kimberly.Germain@cookcountyil.gov>, Kimberly Gouwens (Sheriff)
<Kimberly.Gouwens@cookcountyil.gov>, Krzysztof Piech (Sheriff)
<Krzysztof.Piech@cookcountyil.gov>, Krzysztof Wantuch (Sheriff)
<Krzysztof.Wantuch@cookcountyil.gov>, Kyle Kelley (Sheriff)
<Kyle.Kelley@cookcountyil.gov>, Kyle Sellers (Sheriff)
<Kyle.Sellers2@cookcountyil.gov>, Lakesha Palomino (Sheriff)
<Lakesha.Palomino@cookcountyil.gov>, Lasean Miller (Sheriff)
<LaSean.Miller@cookcountyil.gov>, Lashawn Simmons (Sheriff)
<Lashawn.Simmons@cookcountyil.gov>, Latonya Boyette (Sheriff)
<Latonya.Boyette@cookcountyil.gov>, Latrice Rattler (Sheriff)
<Latrice.Rattler@cookcountyil.gov>, Latrice Thomas (Sheriff)
<Latrice.Thomas@cookcountyil.gov>, Laura Becker (Sheriff)
<Laura.Becker@cookcountyil.gov>, Lauren Langland (Sheriff)
<Lauren.Langland@cookcountyil.gov>, Lawrence O'Rourke (Sheriff)
<lawrence.orourke@cookcountyil.gov>, Leanna Carlson (Sheriff)
<Leanna.Carlson@cookcountyil.gov>, Leanne Hovey (Sheriff)
<Leanne.Hovey@cookcountyil.gov>, Leone Ugarte Avila (Sheriff)
<Leone.UgarteAvila@cookcountyil.gov>, Leslie Pratts (Sheriff)
<Leslie.Pratts@cookcountyil.gov>, Lester Rodgers (Sheriff)
<Lester.Rodgers@cookcountyil.gov>, Levita Perkins (Sheriff)
<Levita.Perkins@cookcountyil.gov>, Lina Rackauskaite (Sheriff)
<Lina.Rackauskaite@cookcountyil.gov>, Linda Olinski (Sheriff)
<Linda.Olinski@cookcountyil.gov>, Lisa Farinella (Sheriff)
<Lisa.Farinella@cookcountyil.gov>, Lisa Garza (Sheriff)
<Lisa.Garza@cookcountyil.gov>, Lissette Rivera (Sheriff)
<Lissette.Rivera@cookcountyil.gov>, L'mekka Edwards (Sheriff)
<lmekka.edwards@cookcountyil.gov>, Lori Hernandez (Sheriff)
<Lori.Hernandez@cookcountyil.gov>, Louie Goros (Sheriff)
<Louie.Goros@cookcountyil.gov>, Luis Blanco (Sheriff)
<Luis.Blanco@cookcountyil.gov>, Luis Domenech (Sheriff)
<Luis.Domenech@cookcountyil.gov>, Luis Santoyo (Sheriff)
<Luis.Santoyo@cookcountyil.gov>, Luz Evelia Serrano (Sheriff)
<LuzEvelia.Serrano@cookcountyil.gov>, Patrick Dwyer (Sheriff)
<Patrick.Dwyer@cookcountyil.gov>

Sent: June 30, 2020 8:07:20 AM CDT

Received: June 30, 2020 8:07:23 AM CDT

Attachments: (U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

Please see the attached DHS Intelligence Brief, “Criminal Hackers Target US Law Enforcement Data,” dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support

resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

If you no longer wish to be on this distribution list, please send an email to ccso.intel@cookcountyil.gov to discontinue receiving these emails. If you would like any member under your command to receive these emails, please send an email to ccso.intel@cookcountyil.gov and include their name, title and email address in the body of the request.

Cook County Sheriff's Office
Strategic Operations Center
3026 S. California Avenue
Building 5, 2nd Floor
Chicago, IL. 60608
Office: 773-674-2694 or 8477
Fax: 773-674-4797

THIS IS A CONFIDENTIAL LAW ENFORCEMENT COMMUNICATION. The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential. If you are not the intended recipient of this message, or if this message has been addressed to you in error, please immediately alert the sender by reply e-mail and then delete this message and its attachments. Do not deliver, distribute, transmit or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action relative to the information contained in this communication and/or attachments. This e-mail and any attached documents may contain For Official Use Only and/or Law Enforcement Sensitive material and should not be disseminated outside of official law enforcement channels. The information contained in this message as well as any attachments shall not be released to the media or the general public.

FW: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>
To:	Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>
Sent:	June 30, 2020 8:07:29 AM CDT
Received:	June 30, 2020 8:07:30 AM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

From: CCSO Intel (Sheriff)
Sent: Tuesday, June 30, 2020 8:07:20 AM (UTC-06:00) Central Time (US & Canada)
Subject: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

Please see the attached DHS Intelligence Brief, "Criminal Hackers Target US Law Enforcement Data," dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

If you no longer wish to be on this distribution list, please send an email to ccso.intel@cookcountyil.gov to discontinue receiving these emails. If you would like any member under your command to receive these emails, please send an email to ccso.intel@cookcountyil.gov and include their name, title and email address in the body of the request.

Cook County Sheriff's Office
Strategic Operations Center
3026 S. California Avenue
Building 5, 2nd Floor
Chicago, IL. 60608
Office: 773-674-2694 or 8477
Fax: 773-674-4797

THIS IS A CONFIDENTIAL LAW ENFORCEMENT COMMUNICATION. The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential. If you are not the intended recipient of this message, or if this message has been addressed to you in error, please immediately alert the sender by reply e-mail and then delete this message and its attachments. Do not deliver, distribute, transmit or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action relative to the information contained in this communication and/or attachments. This e-mail and any attached documents may contain For Official Use Only and/or Law Enforcement Sensitive material and should not be disseminated outside of official law enforcement channels. The information contained in this message as well as any attachments shall not be released to the media or the general public.

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Yolanda Collins-Watson (Sheriff)
Sent:	June 30, 2020 8:07:45 AM CDT
Received:	June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Todd Rohl (Sheriff)
Sent:	June 30, 2020 8:07:45 AM CDT
Received:	June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Walter Klinger (Sheriff)
Sent:	June 30, 2020 8:07:45 AM CDT
Received:	June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Patricia Montgomery-Echols (Sheriff)
Sent:	June 30, 2020 8:07:45 AM CDT
Received:	June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Michael Goldsmith (Sheriff)
Sent: June 30, 2020 8:07:45 AM CDT
Received: June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Nathan Camer (Sheriff)
Sent: June 30, 2020 8:07:45 AM CDT
Received: June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Timothy O'Donnell (Sheriff)
Sent:	June 30, 2020 8:07:45 AM CDT
Received:	June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Tarra Daniels-Davis (Sheriff)
Sent:	June 30, 2020 8:07:45 AM CDT
Received:	June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Randall Pochie (Sheriff)
Sent:	June 30, 2020 8:07:45 AM CDT
Received:	June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Patrick Dwyer (Sheriff)
Sent:	June 30, 2020 8:07:45 AM CDT
Received:	June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Rebecca Dejesus (Sheriff)
Sent: June 30, 2020 8:07:45 AM CDT
Received: June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To: Matthew Goral (Sheriff)
Sent: June 30, 2020 8:07:45 AM CDT
Received: June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Martin Bennett (Sheriff)
Sent:	June 30, 2020 8:07:45 AM CDT
Received:	June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Stavone McHerron (Sheriff)
Sent:	June 30, 2020 8:07:45 AM CDT
Received:	June 30, 2020 8:07:51 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Richard O'Brien (Sheriff)
Sent:	June 30, 2020 8:07:45 AM CDT
Received:	June 30, 2020 8:07:50 AM CDT

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From: CCSO Intel (Sheriff) <CCSO.INTEL@cookcountyil.gov>

Bcc: Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov>, Marcin Szczerbiak (Sheriff) <Marcin.Szczerbiak@cookcountyil.gov>, Marcus Bradfield (Sheriff) <Marcus.Bradfield@cookcountyil.gov>, Margie Sullivan (Sheriff) <Margie.Sullivan@cookcountyil.gov>, Marguerite McCluskey (Sheriff) <Marguerite.McCluskey@cookcountyil.gov>, Maria Lopez (Sheriff) <Maria.Lopez@cookcountyil.gov>, Marie Jeffries (Sheriff) <Marie.Jeffries@cookcountyil.gov>, Mario Ponce (Sheriff) <Mario.Ponce@cookcountyil.gov>, Marissa Sanchez (Sheriff) <Marissa.Sanchez@cookcountyil.gov>, Marissa SanchezKrug (Sheriff) <Marissa.SanchezKrug@cookcountyil.gov>, Mark Mendoza (Sheriff) <Mark.Mendoza@cookcountyil.gov>, Mark Smith (Sheriff) <Mark.Smith@cookcountyil.gov>, Marlon Parks (Sheriff) <Marlon.Parks@cookcountyil.gov>, Marshan Johnson (Sheriff) <Marshan.Johnson@cookcountyil.gov>, Martin Bennett (Sheriff) <Martin.Bennett@cookcountyil.gov>, Martin Hart (Sheriff) <Martin.Hart@cookcountyil.gov>, Martin Juppe (Sheriff) <Martin.Juppe@cookcountyil.gov>, Martin Lukasik (Sheriff) <Martin.Lukasik@cookcountyil.gov>, Martin Webster (Sheriff) <Martin.Webster@cookcountyil.gov>, Mary Przybylski (Sheriff) <Mary.Przybylski@cookcountyil.gov>, Mary.Tamme@cookcountyil.gov, Matthew Brown (Sheriff) <Matthew.Brown@cookcountyil.gov>, Matthew Carlson (Sheriff) <Matthew.Carlson@cookcountyil.gov>, Matthew Coffey (Sheriff) <Matthew.Coffey@cookcountyil.gov>, Matthew Gena (Sheriff) <Matthew.Gena@cookcountyil.gov>, Matthew Goral (Sheriff) <Matthew.Goral@cookcountyil.gov>, Matthew Rafferty (Sheriff) <Matthew.Rafferty@cookcountyil.gov>, Matthew Walsh (Sheriff) <Matthew.Walsh@cookcountyil.gov>, Matthias Vlahos (Sheriff) <Matthias.Vlahos@cookcountyil.gov>, Maureen Donohoe (Sheriff) <Maureen.Donohoe@cookcountyil.gov>, Maurice Ashford (Sheriff) <Maurice.Ashford@cookcountyil.gov>, Maurice Cernick (Sheriff) <Maurice.Cernick@cookcountyil.gov>, Megan Kinsella (Sheriff) <Megan.Kinsella@cookcountyil.gov>, Michael Anton (Sheriff) <Michael.Anton@cookcountyil.gov>, Michael Callahan (Sheriff) <Michael.Callahan1@cookcountyil.gov>, MIchael Cokeley (Sheriff) <Michael.Cokeley@cookcountyil.gov>, Michael Contreras (Sheriff) <Michael.Contreras@cookcountyil.gov>, Michael Dwyer (Sheriff) <Michael.Dwyer@cookcountyil.gov>, Michael Elsen (Sheriff) <Michael.Elsen@cookcountyil.gov>, Michael Fonseca (Sheriff) <Michael.Fonseca@cookcountyil.gov>, Michael Gleason (Sheriff) <Michael.Gleason@cookcountyil.gov>, Michael Gniedziejko (Sheriff) <Michael.Gniedziejko@cookcountyil.gov>, Michael Goldsmith (Sheriff) <Michael.Goldsmith@cookcountyil.gov>, Michael Gomez (Sheriff) <Michael.Gomez@cookcountyil.gov>, Michael Healy (Sheriff) <Michael.Healy@cookcountyil.gov>, Michael Holewinski (Sheriff) <Michael.Holewinski@cookcountyil.gov>, Michael Juraszek (Sheriff) <Michael.Juraszek@cookcountyil.gov>, Michael Kane (Sheriff) <Michael.Kane@cookcountyil.gov>, Michael Kizaric (Sheriff) <Michael.Kizaric@cookcountyil.gov>, Michael Knighton (Sheriff) <Michael.Knighton@cookcountyil.gov>, Michael Kruzel (Sheriff) <Michael.Kruzel@cookcountyil.gov>, Michael Lucente (Sheriff) <Michael.Lucente@cookcountyil.gov>, Michael Mendez (Sheriff) <Michael.Mendez@cookcountyil.gov>, Michael Murphy (Sheriff) <Michael.Murphy2@cookcountyil.gov>, Michael Murphy1 (Sheriff) <Michael.Murphy@cookcountyil.gov>, Michael Parks (Sheriff) <Michael.Parks@cookcountyil.gov>, Michael Quan (Sheriff) <Michael.Quan@cookcountyil.gov>, Michael Raab (Sheriff) <Michael.Raab@cookcountyil.gov>, Michael Rivers (Sheriff) <Michael.Rivers@cookcountyil.gov>, Michael Schaffer (Sheriff) <Michael.Schaffer@cookcountyil.gov>, Michael Sisco (Sheriff)

<Michael.Sisco@cookcountyil.gov>, Michael Storino (Sheriff)
<Michael.Storino@cookcountyil.gov>, Michael Ware (Sheriff)
<Michael.Ware2@cookcountyil.gov>, Michael Ware (Sheriff)
<Michael.Ware@cookcountyil.gov>, Michelle Allen (Sheriff)
<Michelle.Allen@cookcountyil.gov>, Michelle Dorn (Sheriff)
<Michelle.Dorn@cookcountyil.gov>, Michelle Jagielko (Sheriff)
<Michelle.Jagielko@cookcountyil.gov>, Michelle Kaechele (Sheriff)
<Michelle.Kaechele@cookcountyil.gov>, Milan Stojkovic (Sheriff)
<Milan.Stojkovic@cookcountyil.gov>, Mildred Valenzuela (Sheriff)
<Mildred.Valenzuela@cookcountyil.gov>, Mirella Delgado (Sheriff)
<Mirella.Delgado@cookcountyil.gov>, Miriam Bernal (Sheriff)
<Miriam.Bernal@cookcountyil.gov>, Mizell Walls (Sheriff)
<Mizell.Walls@cookcountyil.gov>, Mohammed Akhtar (Sheriff)
<Mohammed.Akhtar@cookcountyil.gov>, Myron Weres (Sheriff)
<Myron.Weres@cookcountyil.gov>, Naima Howard (Sheriff)
<Naima.Howard@cookcountyil.gov>, Nancy Pavelka (Sheriff)
<Nancy.Pavelka@cookcountyil.gov>, Natasha Allen-Victor (Sheriff)
<Natasha.Allen-Victor2@cookcountyil.gov>, Natasha Williams (Sheriff)
<Natasha.Williams@cookcountyil.gov>, Nathan Bowens (Sheriff)
<Nathan.Bowens@cookcountyil.gov>, Nathan Camer (Sheriff)
<Nathan.Camer@cookcountyil.gov>, Nelson Lewis (Sheriff)
<Nelson.Lewis@cookcountyil.gov>, Nicholas Bohlsen (Sheriff)
<Nicholas.Bohlsen@cookcountyil.gov>, Nicholas Trinidad (Sheriff)
<Nicholas.Trinidad@cookcountyil.gov>, Nick Karlos (Sheriff)
<Nick.Karlos@cookcountyil.gov>, Nicole Gordon (Sheriff)
<Nicole.Gordon@cookcountyil.gov>, Nicole Valerio (Sheriff)
<Nicole.Valerio@cookcountyil.gov>, Nik Trzinski (Sheriff)
<Nik.Trzinski@cookcountyil.gov>, Nikolas Hadjian (Sheriff)
<Nikolas.Hadjian@cookcountyil.gov>, Noel Perez (Sheriff)
<Noel.Perez@cookcountyil.gov>, Pablo Trujillo (Sheriff)
<Pablo.Trujillo@cookcountyil.gov>, Pamela Harrington (Sheriff)
<Pamela.Harrington@cookcountyil.gov>, Pamela Williams (Sheriff)
<Pamela.Williams@cookcountyil.gov>, Pascal Waller (Sheriff)
<Pascal.Waller@cookcountyil.gov>, Patricia Duffy (Sheriff)
<Patricia.Duffy@cookcountyil.gov>, Patricia Montgomery-Echols (Sheriff)
<Patricia.Montgomery-echols@cookcountyil.gov>, Patrick Barbella (Sheriff)
<Patrick.Barbella@cookcountyil.gov>, Patrick Brosnan (Sheriff)
<Patrick.Brosnan@cookcountyil.gov>, Patrick Donovan (Sheriff)
<Patrick.Donovan@cookcountyil.gov>, Patrick Doyle (Sheriff)
<Patrick.Doyle@cookcountyil.gov>, Patrick Dwyer (Sheriff)
<Patrick.Dwyer@cookcountyil.gov>, Patrick Hurley (Sheriff)
<Patrick.Hurley@cookcountyil.gov>, Patrick Julian (Sheriff)
<Patrick.Julian@cookcountyil.gov>, Patrick Murray (Sheriff)
<Patrick.Murray@cookcountyil.gov>, Patrina McCoy (Sheriff)
<Patrina.Mccoy@cookcountyil.gov>, Paul Huss (Sheriff)
<Paul.Huss@cookcountyil.gov>, Paul Martinez (Sheriff)
<Paul.Martinez@cookcountyil.gov>, Paul Riley (Sheriff)
<Paul.Riley@cookcountyil.gov>, Paulina Gorzkowska (Sheriff)
<Paulina.Gorzkowska@cookcountyil.gov>, Penny Mateck-Greene (Sheriff)
<Penny.Mateck-Greene@cookcountyil.gov>, Perry Triveri (Sheriff)
<Perry.Triveri@cookcountyil.gov>, Peter Boubourekas (Sheriff)
<Peter.Boubourekas@cookcountyil.gov>, Peter Raines (Sheriff)
<Peter.Raines@cookcountyil.gov>, Philip Fraticola (Sheriff)
<Philip.Fraticola@cookcountyil.gov>, Philip Lapuma (Sheriff)
<Philip.Lapuma@cookcountyil.gov>, Philip Metcalf (Sheriff)
<Philip.Metcalf@cookcountyil.gov>, Phillip Mackey (Sheriff)
<Phillip.Mackey@cookcountyil.gov>, Quiana Washington (Sheriff)
<Quiana.Washington@cookcountyil.gov>, Rachel Koch (Sheriff)
<Rachel.Koch2@cookcountyil.gov>, Rafael Ruiz (Sheriff)
<Rafael.Ruiz@cookcountyil.gov>, Ramon Del Valle (Sheriff)
<Ramon.Delvalle@cookcountyil.gov>, Randa Abuteen (Sheriff)
<Randa.Abuteen@cookcountyil.gov>, Randall Pochie (Sheriff)
<Randall.Pochie@cookcountyil.gov>, Randall Quill (Sheriff)

<Randall.Quill@cookcountyil.gov>, Raul Garcia (Sheriff)
<Raul.Garcia2@cookcountyil.gov>, Raymond Struck (Sheriff)
<Raymond.Struck@cookcountyil.gov>, Rebecca Cancellare (Sheriff)
<Rebecca.Cancellare@cookcountyil.gov>, Rebecca Coughlin (Sheriff)
<Rebecca.Coughlin@cookcountyil.gov>, Rebecca Dejesus (Sheriff)
<Rebecca.Dejesus@cookcountyil.gov>, Rebecca Llanes (Sheriff)
<Rebecca.Llanes@cookcountyil.gov>, Renee Richardson (Sheriff)
<Renee.Richardson@cookcountyil.gov>, Renee Smith (Sheriff)
<Renee.Smith@cookcountyil.gov>, Rex Knaperek (Sheriff)
<Rex.Knaperek@cookcountyil.gov>, Ricardo Hardy (Sheriff)
<Ricardo.Hardy@cookcountyil.gov>, Ricardo Ibarra (Sheriff)
<Ricardo.Ibarra@cookcountyil.gov>, Richard Delavega (Sheriff)
<Richard.Delavega@cookcountyil.gov>, Richard Garcia1 (Sheriff)
<Richard.Garcia2@cookcountyil.gov>, Richard Jurgens (Sheriff)
<Richard.Jurgens@cookcountyil.gov>, Richard Liboy (Sheriff)
<Richard.Liboy@cookcountyil.gov>, Richard O'Brien1 (Sheriff)
<Richard.O'brien2@cookcountyil.gov>, Richard Petersen (Sheriff)
<Richard.Petersen@cookcountyil.gov>, Richard Urso (Sheriff)
<Richard.Urso@cookcountyil.gov>, Richard Velasquez (Sheriff)
<Richard.Velasquez@cookcountyil.gov>, Rikki Johnson (Sheriff)
<Rikki.Johnson@cookcountyil.gov>, Rita Mendez (Sheriff)
<Rita.Mendez@cookcountyil.gov>, Robert Almeida (Sheriff)
<Robert.Almeida@cookcountyil.gov>, Robert Bonakowski (Sheriff)
<Robert.Bonakowski@cookcountyil.gov>, Robert Cassidy (Sheriff)
<Robert.Cassidy@cookcountyil.gov>, Robert Devogelear (Sheriff)
<Robert.Devogelear@cookcountyil.gov>, Robert Gassmann (Sheriff)
<Robert.Gassmann@cookcountyil.gov>, Robert Hausherr (Sheriff)
<Robert.Hausherr@cookcountyil.gov>, Robert Lobacz (Sheriff)
<Robert.Lobacz@cookcountyil.gov>, Robert Mousel (Sheriff)
<Robert.Mousel@cookcountyil.gov>, Robert O'Neill (Sheriff)
<Robert.O'Neill@cookcountyil.gov>, Robert Ortiz (Sheriff)
<Robert.Ortiz@cookcountyil.gov>, Robert Ruminski (Sheriff)
<Robert.Ruminski@cookcountyil.gov>, Robert Ryjewski (Sheriff)
<Robert.Ryjewski@cookcountyil.gov>, Robert Waller (Sheriff)
<Robert.Waller@cookcountyil.gov>, Robert Zivalich (Sheriff)
<Robert.Zivalich@cookcountyil.gov>, Rochelle Parker (Sheriff)
<Rochelle.Parker@cookcountyil.gov>, Roderick Kirkwood (Sheriff)
<Roderick.Kirkwood@cookcountyil.gov>, Roderick Pierce (Sheriff)
<Roderick.Pierce@cookcountyil.gov>, Roger Comer (Sheriff)
<Roger.Comer@cookcountyil.gov>, Roger Guerra (Sheriff)
<Roger.Guerra@cookcountyil.gov>, Ronald Prohaska (Sheriff)
<Ronald.Prohaska@cookcountyil.gov>, Ronald Sachtleben (Sheriff)
<Ronald.Sachtleben@cookcountyil.gov>, Ronald Szura (Sheriff)
<Ronald.Szura@cookcountyil.gov>, Roy Jones (Sheriff)
<Roy.Jones@cookcountyil.gov>, Ruben Rangel (Sheriff)
<Ruben.Rangel@cookcountyil.gov>, Ruben Salazar (Sheriff)
<Ruben.Salazar@cookcountyil.gov>, Ruth Mendez (Sheriff)
<Ruth.Mendez@cookcountyil.gov>, Ryan George (Sheriff)
<Ryan.George@cookcountyil.gov>, Ryan Huber (Sheriff)
<Ryan.Huber@cookcountyil.gov>, Ryan Killacky (Sheriff)
<Ryan.Killacky@cookcountyil.gov>, Sajid Haidari (Sheriff)
<Sajid.Haidari@cookcountyil.gov>, Salvatore Marra (Sheriff)
<Salvatore.Marra@cookcountyil.gov>, Samina Alva (Sheriff)
<Samina.Alva@cookcountyil.gov>, Samina Bonilla (Sheriff)
<Samina.Bonilla@cookcountyil.gov>, Samuel Cory (Sheriff)
<Samuel.Cory@cookcountyil.gov>, Samuel Senerchia (Sheriff)
<Samuel.Senerchia@cookcountyil.gov>, Samuel Suffern (Sheriff)
<Samuel.Suffern@cookcountyil.gov>, Sandra Crespo Hernandez (Sheriff)
<Sandra.CrespoHernandez@cookcountyil.gov>, Sang Yi (Sheriff)
<Sang.Yi@cookcountyil.gov>, Santiono Dyer (Sheriff)
<Santiono.Dyer@cookcountyil.gov>, Santo Duffy (Sheriff)
<Santo.Duffy@cookcountyil.gov>, Scott Giertuga (Sheriff)
<Scott.Giertuga@cookcountyil.gov>, Scott Gordon (Sheriff)

<Scott.Gordon@cookcountyil.gov>, Scott Lefko (Sheriff)
<Scott.Lefko@cookcountyil.gov>, Sean Gleason (Sheriff)
<Sean.Gleason@cookcountyil.gov>, Sean Kelly (Sheriff)
<Sean.Kelly2@cookcountyil.gov>, Sean Murphy (Sheriff)
<Sean.Murphy@cookcountyil.gov>, Sebastian Golik (Sheriff)
<Sebastian.Golik@cookcountyil.gov>, Servando Velez (Sheriff)
<Servando.Velez@cookcountyil.gov>, Sharon Ustaszewski (Sheriff)
<Sharon.Ustaszewski@cookcountyil.gov>, Shaunna Rozhon (Sheriff)
<Shaunna.Rozhon@cookcountyil.gov>, Shawn Knapp (Sheriff)
<Shawn.Knapp@cookcountyil.gov>, Shawn Murphy (Sheriff)
<Shawn.Murphy@cookcountyil.gov>, Shelly Hendricks (Sheriff)
<Shelly.Hendricks@cookcountyil.gov>, Shenita Thomas (Sheriff)
<Shenita.Thomas@cookcountyil.gov>, Sheree Clark (Sheriff)
<Sheree.Clark@cookcountyil.gov>, Shereen Gamble (Sheriff)
<Shereen.Gamble1@cookcountyil.gov>, Sheri Holler (Sheriff)
<Sheri.Holler@cookcountyil.gov>, Sherod Craig (Sheriff)
<Sherod.Craig@cookcountyil.gov>, Sheryl Collins (Sheriff)
<Sheryl.Collins@cookcountyil.gov>, Shirley McGreal (Sheriff)
<Shirley.Mcgreal@cookcountyil.gov>, Sonya Delove (Sheriff)
<Sonya.DeLove@cookcountyil.gov>, Stacey Mc Queary (Sheriff)
<Stacey.Mcqueary@cookcountyil.gov>, Stavone McHerron (Sheriff)
<Stavone.Mcherron@cookcountyil.gov>, Stephen Moody (Sheriff)
<Stephen.Moody@cookcountyil.gov>, Steven Bialczak (Sheriff)
<Steven.Bialczak@cookcountyil.gov>, Steven Blazina (Sheriff)
<Steven.Blazina@cookcountyil.gov>, Steven Martino (Sheriff)
<Steven.Martino@cookcountyil.gov>, Steven Williams (Sheriff)
<Steven.Williams@cookcountyil.gov>, Steven Zepeda (Sheriff)
<Steven.Zepeda@cookcountyil.gov>, Susan Collum (Sheriff)
<Susan.Collum@cookcountyil.gov>, Susano Viramontes (Sheriff)
<Susano.Viramontes@cookcountyil.gov>, Tamara Levickas (Sheriff)
<Tamara.Levickas@cookcountyil.gov>, Tamera Jones (Sheriff)
<Tamera.Jones@cookcountyil.gov>, Tanda Adams (Sheriff)
<Tanda.Adams@cookcountyil.gov>, Tangenise Porter (Sheriff)
<Tangenise.Porter@cookcountyil.gov>, Tarra Daniels-Davis (Sheriff)
<Tarra.Daniels-Davis@cookcountyil.gov>, Taylor Boldt (Sheriff)
<Taylor.Boldt@cookcountyil.gov>, Ted Sakelaris (Sheriff)
<Ted.Sakelaris@cookcountyil.gov>, Teresa Ruiz (Sheriff)
<Teresa.Ruiz@cookcountyil.gov>, Teresa Serna (Sheriff)
<Teresa.Serna@cookcountyil.gov>, Terese Cruz (Sheriff)
<Terese.Cruz@cookcountyil.gov>, Terra Martin (Sheriff)
<Terra.Martin@cookcountyil.gov>, Terrell Andrews (Sheriff)
<Terrell.Andrews@cookcountyil.gov>, Terrence Doran (Sheriff)
<Terrence.Doran@cookcountyil.gov>, Terrence O'Driscoll (Sheriff)
<Terrence.O'Driscoll@cookcountyil.gov>, Terrence Ross (Sheriff)
<Terrence.Ross@cookcountyil.gov>, Terrence Tabb (Sheriff)
<Terrence.Tabb@cookcountyil.gov>, Terrence Whittler (Sheriff)
<Terrence.Whittler@cookcountyil.gov>, Theodore Stajura (Sheriff)
<Theodore.Stajura@cookcountyil.gov>, Theodore Williams (Sheriff)
<Theodore.Williams@cookcountyil.gov>, Theresa Hermann (Sheriff)
<Theresa.Hermann@cookcountyil.gov>, Theresa Trinidad (Sheriff)
<Theresa.Trinidad@cookcountyil.gov>, Thomas Albright (Sheriff)
<Thomas.Albright@cookcountyil.gov>, Thomas Burke (Sheriff)
<Thomas.Burke@cookcountyil.gov>, Thomas Clemmons (Sheriff)
<Thomas.Clemmons@cookcountyil.gov>, Thomas Maciunas (Sheriff)
<Thomas.Maciunas@cookcountyil.gov>, Thomas Mc Inerney (Sheriff)
<Thomas.Mcinerney@cookcountyil.gov>, Thomas McQuaid (Sheriff)
<Thomas.Mcquaid@cookcountyil.gov>, Thomas Nortman (Sheriff)
<Thomas.Nortman@cookcountyil.gov>, Thomas Shader (Sheriff)
<Thomas.Shader@cookcountyil.gov>, Thomas Sinks (Sheriff)
<Thomas.Sinks@cookcountyil.gov>, Tiffany Nagel (Sheriff)
<Tiffany.Nagel2@cookcountyil.gov>, Timothy Bergel (Sheriff)
<Timothy.Bergel@cookcountyil.gov>, Timothy Hannigan (Sheriff)
<Timothy.Hannigan@cookcountyil.gov>, Timothy Mc Phillips (Sheriff)

<Timothy.Mcphillips@cookcountyil.gov>, Timothy Murray (Sheriff)
<Timothy.Murray@cookcountyil.gov>, Timothy O'Donnell (Sheriff)
<Timothy.O'donnell@cookcountyil.gov>, Timothy Popp (Sheriff)
<Timothy.Popp@cookcountyil.gov>, Todd Lukas (Sheriff)
<Todd.Lukas@cookcountyil.gov>, Todd Rohl (Sheriff)
<Todd.Rohl@cookcountyil.gov>, Toia Sappington (Sheriff)
<Toia.Sappington@cookcountyil.gov>, Tomas Perez (Sheriff)
<Tomas.Perez@cookcountyil.gov>, Tomasz Tustanowski (Sheriff)
<Tomasz.Tustanowski@cookcountyil.gov>, Tommie Hall (Sheriff)
<Tommie.Hall@cookcountyil.gov>, Tommy Koniewicz (Sheriff)
<Tommy.Koniewicz@cookcountyil.gov>, Tony Wasco (Sheriff)
<Tony.Wasco@cookcountyil.gov>, Tracy Clopton (Sheriff)
<Tracy.Clopton@cookcountyil.gov>, Tracy O'Donnell (Sheriff)
<Tracy.ODonnell@cookcountyil.gov>, Troy Smith (Sheriff)
<Troy.Smith@cookcountyil.gov>, Valerie Gorniak (Sheriff)
<Valerie.Gorniak@cookcountyil.gov>, Vernon Jackson (Sheriff)
<Vernon.Jackson@cookcountyil.gov>, Veronica Roman (Sheriff)
<Veronica.Roman@cookcountyil.gov>, Victor Marin (Sheriff)
<Victor.Marin@cookcountyil.gov>, Victor Siedleski (Sheriff)
<Victor.Siedleski@cookcountyil.gov>, Victor Van Horn (Sheriff)
<Victor.Vanhorn@cookcountyil.gov>, Viktor Yatsyk (Sheriff)
<Viktor.Yatsyk@cookcountyil.gov>, Vincent Gamez (Sheriff)
<Vincent.Gamez@cookcountyil.gov>, Vincent Garrett (Sheriff)
<Vincent.Garrett@cookcountyil.gov>, Vincent Greene (Sheriff)
<Vincent.Greene@cookcountyil.gov>, Walter Klinger (Sheriff)
<Walter.Klinger@cookcountyil.gov>, Wanda Barnes (Sheriff)
<Wanda.Barnes@cookcountyil.gov>, Wanda Cintron (Sheriff)
<Wanda.Cintron@cookcountyil.gov>, Wanda Walker (Sheriff)
<Wanda.Walker@cookcountyil.gov>, Warrick Graham (Sheriff)
<Warrick.Graham3@cookcountyil.gov>, Wilfrido Trejo (Sheriff)
<Wilfrido.Trejo@cookcountyil.gov>, William De La Fuente (Sheriff)
<William.Delafuente@cookcountyil.gov>, William Evers (Sheriff)
<William.Evers@cookcountyil.gov>, William Hoefler (Sheriff)
<William.Hoefler@cookcountyil.gov>, William Jackson (Sheriff)
<William.Jackson1@cookcountyil.gov>, William Jones (Sheriff)
<William.Jones@cookcountyil.gov>, William Leen (Sheriff)
<William.Leen@cookcountyil.gov>, William Mak (Sheriff)
<William.Mak@cookcountyil.gov>, William Moran (Sheriff)
<William.Moran@cookcountyil.gov>, William O'Mary (Sheriff)
<William.O'Mary@cookcountyil.gov>, William Smith (Sheriff)
<William.Smith@cookcountyil.gov>, Willie Lewis (Sheriff)
<Willie.Lewis@cookcountyil.gov>, Winston Geralds (Sheriff)
<Winston.Geralds@cookcountyil.gov>, Wyees Williams (Sheriff)
<Wyees.Williams@cookcountyil.gov>, Yamile NoaSerna (Sheriff)
<Yamile.NoaSerna@cookcountyil.gov>, Yashira Rivas (Sheriff)
<Yashira.Rivas@cookcountyil.gov>, Yolanda Collins-Watson (Sheriff)
<Yolanda.Collins-Watson@cookcountyil.gov>, Zachary Almaoui (Sheriff)
<Zachary.Almaoui@cookcountyil.gov>, Zachary Smith (Sheriff)
<Zachary.Smith@cookcountyil.gov>

Sent: June 30, 2020 8:07:45 AM CDT

Received: June 30, 2020 8:07:47 AM CDT

Attachments: (U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

Please see the attached DHS Intelligence Brief, “Criminal Hackers Target US Law Enforcement Data,” dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

If you no longer wish to be on this distribution list, please send an email to ccso.intel@cookcountyil.gov to discontinue receiving these emails. If you would like any member under your command to receive these emails, please send an email to ccso.intel@cookcountyil.gov and include their name, title and email address in the body of the request.

Cook County Sheriff's Office
Strategic Operations Center
3026 S. California Avenue
Building 5, 2nd Floor
Chicago, IL. 60608
Office: 773-674-2694 or 8477
Fax: 773-674-4797

THIS IS A CONFIDENTIAL LAW ENFORCEMENT COMMUNICATION. The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential. If you are not the intended recipient of this message, or if this message has been addressed to you in error, please immediately alert the sender by reply e-mail and then delete this message and its attachments. Do not deliver, distribute, transmit or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action relative to the information contained in this communication and/or attachments. This e-mail and any attached documents may contain For Official Use Only and/or Law Enforcement Sensitive material and should not be disseminated outside of official law enforcement channels. The information contained in this message as well as any attachments shall not be released to the media or the general public.

[Heads Up] How Slack Phishing Works - The Latest Tricky Attack Vector

From: CyberheistNews <donotreply@cyberheistnews.com>
To: adnan.memon@cookcountyil.gov, Adnan Memon (Sheriff) <Adnan.Memon@cookcountyil.gov>

Sent: June 30, 2020 8:31:54 AM CDT
Received: June 30, 2020 8:32:12 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

[Heads Up] How Slack Phishing Works - The Latest Tricky Attack Vector

Email not displaying? | View Knowbe4 Blog

Unsubscribe

CyberheistNews Vol 10 #27 | June 30th., 2020

[Heads Up] How Slack Phishing Works - The Latest Tricky Attack Vector

People need to be able to use their instincts in order to spot new phishing techniques, according to Ashley Graves, a Cloud Security Researcher at AT&T Alien Labs. On the CyberWire's Research Saturday podcast, Graves described a phishing technique that abuses webhooks in Slack to fool users into granting an attacker access to their Slack data.

A webhook is a feature that allows third-party apps to send messages to a specific Slack channel via a unique URL. Anyone can send a message to the Slack channel if they know this URL, so it's important that the URL be kept secret. If an attacker discovers a leaked webhook URL, they can craft a phishing message and send it directly into a Slack workspace to trick a user into installing a malicious app. This app can then exfiltrate data from the targeted workspace.

Graves emphasized that this attack doesn't have any visible warning signs, since the communication comes directly from Slack through a legitimate service.

"The only indication that exists would be the person's gut feeling that it doesn't seem right, that this app should not be requesting this level of data," she said.

Graves said part of the solution is improved awareness around what attackers can do with certain information. "So, I think some people legitimately don't understand how

much access an attacker can gain when credentials are leaked, and even more so when a webhook secret is leaked," Graves explained.

"On the other side of it is understanding what you're giving third parties access to. So, knowing to read those OAuth scopes, understanding how the application that you're using might use that access. Like, it wouldn't make sense – to me, at least – for a webhook to need access to my documents.

So, that's something that they have to look over and have some sort of understanding around whether it's some self-learning, whether it's included in security awareness training or something like that."

Graves noted that anyone can be fooled by social engineering, so companies need to ensure that users know when they should be cautious and ask for assistance before taking an action.

"But again, we've seen in similar attacks in the past that users can be easily tricked and that it's not stupidity," she said. "It's not even ignorance. It's just that this is very new technology to a lot of people, and the prompts are not always clear, and there is a lot of small text about how they work. So I think that companies need to, I suppose, make as much effort as possible to help people understand the impact of their actions."

Attackers will never stop coming up with new ways to dupe people into granting them access. New-school security awareness training can give your employees a healthy sense of suspicion to enable them to stop social engineering attacks.

The CyberWire has the story:
https://thecyberwire.com/podcasts/research-saturday/140/transcript

[Live Demo] Ridiculously Easy Security Awareness Training and Phishing

Old-school awareness training does not hack it anymore. Your email filters have an average 7-10% failure rate; you need a strong human firewall as your last line of defense.

Join us **Wednesday, July 8 @ 2:00 pm (ET),** for a live demonstration of how KnowBe4 introduces a new-school approach to Security Awareness Training and Simulated Phishing.

See how easy it is to train and phish your users:

- Train your users with access to the **world's largest library** of 1000+ pieces of awareness training content.
- Send fully automated **simulated phishing attacks,** including thousands of customizable templates with unlimited usage.
- **NEW! Brandable Content** feature gives you the option to add branded custom content to select training modules.
- **Assessments** allows you to find out where your users are in both **security knowledge** and **security culture** to help establish baseline security metrics you can improve over time.

- **Advanced Reporting** on 60+ key awareness training indicators.
- **Active Directory Integration** to easily upload user data, eliminating the need to manually manage user changes.

Find out how 33,000+ organizations have mobilized their end-users as their human firewall.

Date/Time: **Wednesday, July 8 @ 2:00 pm (ET)**

Save My Spot!

https://event.on24.com/wcc/r/2439681/925D004197E678DDCC946A93B31C24D9?partnerref=CHN2

[ALERT] A New Devilish Malware Worm Called Lucifer Is Targeting Your Windows Workstations

Palo Alto Networks' Unit 42 Security experts have identified a malware worm called Lucifer, that targets Windows systems with cryptojacking and distributed denial-of-service (DDoS) attacks.

This brand-new strain initially tries to infect PCs by bombarding them with a big list of known exploits, hoping to cash in on unpatched vulns. While patches for all these critical and high-severity bugs exist, the organizations infected by this new strain malware had not applied the patches.

"Lucifer is a new hybrid of cryptojacking and DDoS malware variant that leverages old vulnerabilities to spread and perform malicious activities on Windows platforms," Palo Alto said last Wednesday in a blog post. "Applying the updates and patches to the affected software are strongly advised."

The exploits Lucifer is using include Rejetto HTTP File Server (CVE-2014-6287), Oracle Weblogic (CVE-2017-10271), ThinkPHP RCE (CVE-2018-20062), Apache Struts (CVE-2017-9791), Laravel framework CVE-2019-9081), and Microsoft Windows (CVE-2017-0144, CVE-2017-0145, and CVE-2017-8464).

After a successful exploit, the strain connects to its command-and-control (C2) server and is able to execute any commands on the fully pwned device. Some "features" allow the malware to drop an XMRig miner and launch cryptojacking attacks, as well as collecting interface info and sending the miner status to the C2.

The malware is also capable of self-propagation with worm-like features.

The Threatpost site commented: "It scans for either open TCP ports (also known as port 1433) or open Remote Procedure Call (RPC) ports (also known as port 135). If either of these ports is open, the malware attempts to brute-force the login using a default administrator username and an embedded password list (a full list of the passwords used can be found on Unit 42's analysis). It then copies and runs the malware binary on the remote host upon successful authentication.

Please forward to your friends. Blog post with links continued here:

https://blog.knowbe4.com/heads-up-a-new-devilish-malware-worm-called-lucifer-is-targeting-your-windows-workstations

See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments and third-party vendor risk is a continuous problem.

We listened! KCM now has **Compliance, Risk, Policy and Vendor Risk Management** modules, transforming KCM into a full SaaS GRC platform!

Join us **Wednesday, July 8 @ 1:00 PM (ET),** for a 30-minute live product demonstration of KnowBe4's KCM GRC platform. See how you can simplify the challenges of managing your compliance requirements within your organization and across third-party vendors and ease your burden when it's time for risk assessments and audits.

- **NEW!** Demonstrate overall progress and health of your compliance and risk management initiatives with **custom reports.**
- **Vet, manage and monitor** your third-party vendors' security risk requirements.
- **Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.
- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **Wednesday, July 8 @ 1:00 PM (ET)**

Save My Spot!

https://event.on24.com/wcc/r/2439682/58CC9CFF88DA458F08828606604A4E42?partnerref=CHN2

Cyber Crime Uses Adobe and Samsung Servers to Hide Their Phishing Attacks

Researchers at Check Point have observed a phishing campaign that, to avoid detection, abused servers belonging to Adobe, Samsung, and the University of Oxford. The attackers used several layers of deception to disguise their phishing emails as legitimate.

The phishing emails purported to come from Microsoft and informed recipients that

they'd received a voicemail on their Office 365 account. If the user clicked the link in the email, they'd be redirected through a legitimate server before landing on a spoofed Office 365 login page designed to steal their credentials.

The redirection step was accomplished using an Adobe Campaign open redirect link belonging to Samsung Canada, meant for the company's email campaigns. Open redirects enable anyone to craft a URL that will route a user through the server hosting the URL before sending them on to the specified website.

In this case, the attackers used the open redirect link from Samsung's email campaign for Cyber Monday in 2018 and modified it to point to their phishing page.

"The technique of using Adobe Campaign open redirect was initially discovered in September 2019 on the domain belonging to Adobe itself," the researchers write. "In the last few months, it's been widely abused for phishing purposes. To evade detection, attackers abuse open and reputable Adobe Campaign servers to redirect potential victims to their own phishing websites.

This means that the link embedded in the phishing email is part of a trusted domain – one that unknowingly redirects victims to the phishing website."

The attackers also managed to abuse the University of Oxford's email servers to disguise the origin of the emails. "Using legitimate Oxford SMTP servers allowed the attackers to pass the reputation check for the sender domain," Check Point says. "In addition, there was no need to compromise actual email accounts to send phishing emails because they could generate as many email addresses as they wanted."

Finally, the phishing kit itself was hosted on a compromised WordPress site. It would generate a new directory for each visitor, as well as unique, obfuscated source code to avoid detection by security tools.

"The second layer of redirection is used to distance the final phishing page from the original email," the researchers explain. "In this case, the attackers used several compromised WordPress sites which contain malicious redirect code. Introducing another redirection layer enables the attackers to circumvent security solutions that investigate the links within the email.

Thus the URL within the email points to a WordPress site instead of a suspicious-looking phishing page." Attackers will never stop finding new ways to defeat security technologies. New-school security awareness training can give your organization an essential layer of defense by enabling your employees to recognize phishing emails that make it through your filters.

Check Point has the story:
https://research.checkpoint.com/2020/phishing-campaign-exploits-samsung-adobe-and-oxford-servers/

[On-Demand] 10 Incredible Ways You Can Be Hacked Through Email & How to Stop the Bad Guys

Email is still the #1 attack vector the bad guys use. A whopping 91% of cyberattacks start with a phishing email, but email hacking is much more than phishing and launching malware.

In this on-demand webinar Roger A. Grimes, KnowBe4's Data-Driven Defense Evangelist and security expert with over 30-years of experience, explores **10 ways hackers use social engineering to trick your users** into revealing sensitive data or enabling malicious code to run. Plus, he shares a **hacking demo by KnowBe4's Chief Hacking Officer Kevin Mitnick.**

Roger will teach you:

- How silent malware launches, remote password hash capture, and how rogue rules work
- Why rogue documents, establishing fake relationships and getting you to compromise your ethics are so effective
- Details behind clickjacking and web beacons
- Actionable steps on how to defend against them all

If all you were worried about were phishing attempts, think again!
https://info.knowbe4.com/webinar-10-ways-hacked-email

Let's stay safe out there.

Warm Regards,

Stu Sjouwerman
Founder and CEO
KnowBe4, Inc

PS: Just For YOU. We just added 2 new training modules featuring Roger Grimes about data-driven defense:
https://blog.knowbe4.com/new-training-modules-added-on-data-driven-defense

PSS: Need to educate your C-level execs? Here are five cybersecurity books that everyone should —and can— read, recommended by the Wall Street Journal:
https://www.wsj.com/articles/five-cybersecurity-books-that-everyone-shouldand-canread-11592579360

Quotes of the Week

"It is not because things are difficult that we do not dare,
it is because we do not dare that they are difficult."
- Lucius Annaeus Seneca, Philosopher, Statesman, Dramatist (5 BC - 65 AD)

"I am always doing that which I cannot do, in order that I may learn how to do it."

- Pablo Picasso, Artist (1881 - 1973)

Thanks for reading CyberheistNews
But if you want to unsubscribe, you can do that right here

You can read CyberheistNews online at our Blog
https://blog.knowbe4.com/cyberheistnews-vol-10-27-heads-up-how-slack-phishing-works-the-latest-tricky-attack-vector

Security News

Pyongyang's Phishing With Job Offers

An attack campaign with possible ties to North Korea's Lazarus Group targeted aerospace and military companies in Europe and the Middle East with spearphishing attacks late last year, according to researchers at ESET.

The campaign, which the researchers call "Operation In(ter)ception," used social engineering attacks on LinkedIn to trick employees into opening malware-laden documents.

"To initiate contact, they approached the targets with fictitious job offers using LinkedIn's messaging feature," the researchers write. "In order to appear credible, the attackers posed as representatives of well-known, existing companies in the aerospace and defense industry.

For each of the targeted companies we investigated, the attackers had created a separate fake LinkedIn account: one impersonating an HR manager from Collins Aerospace (formerly Rockwell Collins), a major US supplier of aerospace and defense products; the other posing as an HR representative of General Dynamics, another large US-based corporation with a similar focus. "

Interestingly, while the attackers' primary goal was espionage, ESET observed one case in which the attackers used a victim's email account in an attempt to conduct a business email compromise (BEC) scam. While BEC attacks are usually associated with criminals rather than state-sponsored groups, North Korean cyber actors often conduct financially motivated attacks to generate revenue for their heavily sanctioned regime.

"Among the victim's emails, the attackers found communication between the victim and a customer regarding an unresolved invoice," the

researchers explain. “They followed up the conversation and urged the customer to pay the invoice, however, to a different bank account than previously agreed, to which the customer responded with some inquiries.

As part of this ruse, the attackers registered an identical domain name to that of the compromised company, but on a different top-level domain, and used an email associated with this fake domain for further communication with the targeted customer.

The attackers did not respond to the customer’s inquiries and continued to urge them to pay. Instead of paying the invoice, however, the targeted customer reached out to the correct email address of the victim for assistance, thwarting the attackers’ attempt. The victim recognized something was amiss and reported the communication as an incident.”

Sometimes it’s espionage, and sometimes it’s fraud. Recognizing the motive can help recognize the attack. New-school security awareness training can provide your employees with the knowledge they need to thwart targeted social engineering attacks.

ESET has the story:
https://www.welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/

Survey Says...You've Been Pwned

Survey are enticing, and so are survey scams. But they’re easy to recognize if you know what to look for, according to Paul Ducklin at Naked Security.

Ducklin describes a typical survey scam that Sophos spotted recently. The scammers impersonate well-known brands and offer a reward to users that fill out a survey. Real companies use these surveys as well, but the rewards from a legitimate survey are very small, such as a coupon for your next order.

The fake survey asks generic, innocuous questions that could apply to any business, and allows the user to choose their answers from multiple-choice panels. Throughout this process, the site displays the text “38 visitors on this page,” and “6 rewards left” to induce a sense of urgency.

After completing the survey, the user is informed that they’ve actually won an expensive prize, such as a free iPhone.

At the final page, however, it’s revealed that the user will have to pay one

dollar as a delivery fee before they can receive their prize. To do this, they'll be asked to enter their name, address, and credit card information, which will be sent straight to the scammers.

Ducklin stresses that no matter how tempting the deal is, you should leave the site if you sense anything out of place. Even if you don't see any warning signs, the moment a site asks you to enter any sensitive information should be your cue to leave.

"Remember, if you are taking a survey and you see anything that doesn't add up – anything at all – then you need to get off the website right away before you get sucked into giving away any personal information," Ducklin writes.

"Legitimate companies and genuine surveys should be clearly explained in advance, so if the goalposts move halfway through, you're being scammed." Ducklin adds that common sense, awareness, and level-headedness is usually all that's needed to defeat these types of scams.

"There is no free iPhone," he says. "Or Android, or tablet, or laptop. There just isn't. Stores don't hand out $1000 mobile phones in return for you telling them whether you think they should stay open later. They just don't. Follow your head and not your heart."

New-school security awareness training can help your employees recognize social engineering tactics and avoid falling for scams.

Naked Security has the story:
https://nakedsecurity.sophos.com/2020/06/22/anatomy-of-a-survey-scam-how-innocent-questions-can-rip-you-off/

KnowBe4 Announcement: New Training Modules Added on Data-Driven Defense

We have exciting news to share! Two new modules have been released about data-driven defense, both featuring Data-Driven Evangelist Roger Grimes. Join Roger Grimes as he introduces the overall concepts of a risk-analyzed, data-driven computer defense, as conceptualized in his book, A Data-Driven Computer Defense: A Way to Improve Any Computer Defense.

These brand-new modules cover the following:

- An Introduction to Data-Driven Defense: Roger discusses the basic principles behind a data-driven defense and what most companies get wrong about cybersecurity risk and why.

- Data-Driven Defense: Hackers and Why They Hack: Roger discusses the different types of hackers and their motivations. If you're going to fight hackers, it's best if you understand why they hack and what they are after.

You are able to view both modules in the ModStore. Get no-charge access here:
https://blog.knowbe4.com/new-training-modules-added-on-data-driven-defense

The 10 Interesting News Items This Week

1. **This ransomware has learned a new trick: Scanning for point of sales devices:**
 https://www.zdnet.com/article/this-ransomware-has-learned-a-new-trick-scanning-for-point-of-sales-devices/

2. **Black Hat Survey: Breach Concerns Hit Record Levels Due to COVID-19:**
 https://www.darkreading.com/threat-intelligence/black-hat-survey-breach-concerns-hit-record-levels-due-to-covid-19/d/d-id/1338167

3. **Companies Name One of the Biggest Cybersecurity Threats: Their Employees - The Wall Street Journal:**
 https://www.wsj.com/articles/companies-name-one-of-the-biggest-cybersecurity-threats-their-employees-11592606115?

4. **Really good article on security awareness in SC Mag:**
 https://www.scmagazine.com/infosec-world-2020/lululemons-rex-sarabia-works-up-a-sweat-building-a-security-awareness-program-from-scratch/

5. **FBI warns K12 schools of ransomware attacks via RDP:**
 https://www.zdnet.com/article/fbi-warns-k12-schools-of-ransomware-attacks-via-rdp/

6. **Don't Fall Victim to These Common Social Networking Scams. By yours truly at Forbes:**
 https://www.forbes.com/sites/forbestechcouncil/2020/06/24/dont-fall-victim-to-these-common-social-networking-scams/#259d5d6e5462

7. **10 (more) free security tools worth a look via @csoonline:**
 https://www.csoonline.com/article/3563872/10-more-free-security-tools-worth-a-look.html

8. **Hackers abuse Samsung Canada, others, to launch phishing attacks:**
 https://research.checkpoint.com/2020/phishing-campaign-exploits-samsung-adobe-and-oxford-servers/

9. **Ransomware operators lurk on your network after their attack:**
 https://www.bleepingcomputer.com/news/security/ransomware-operators-lurk-on-your-network-after-their-attack/

10. **Ouch. BlueLeaks data dump exposes over 24 years of police records:**
 https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/

Cyberheist 'Fave' Links

This Week's Links We Like, Tips, Hints and Fun Stuff

- **Your Virtual Vacation this week: Eagle Creek Trail - Amazing Trip:**
 https://www.youtube.com/watch?v=T5DzGrDp5Xw

- **41 Next-Level Hotels To Visit Before You Die:**
 https://www.youtube.com/watch?v=FdkxZLfvm6Y

- **Ethiopia's Chapel in the Sky:**
 https://www.youtube.com/watch?v=IJCy64adY3Y

- **44 Things To Add To Your Thrill-Seeking Bucket List:**
 https://www.youtube.com/watch?v=0EPk5o_yvKY

- **How '1917' Was Filmed To Look Like One Shot. Incredible cinematography:**
 https://www.youtube.com/watch?v=kMBnvz-dEXw

- **Danny Macaskill: Mountain Biking Over The Ridge:**
 https://www.flixxy.com/danny-macaskill-mountain-biking-over-the-ridge.htm?utm_source=4

- **Pursuit - A 4K storm time-lapse film:**
 https://www.youtube.com/watch?v=oagszCmJLpU

- **Cats wake up their owner by cute actions:**
 https://www.youtube.com/watch?v=CL1Cdw_wtuk

- **The Golden Retriever Puppy Attack:**
 https://www.youtube.com/watch?v=Lc6db8qfZEw

- **Got a Pest Problem? Call the Quack Squad:**
 https://www.youtube.com/watch?v=H6Ehoxu9QY8

- **For Da Kids #1: How Parrots Express Their Affection:**
 https://www.flixxy.com/how-parrots-express-their-affection.htm?utm_source=4

- **For Da Kids #2: Einstein the African Grey Parrot showed off her vocabulary skills with a 200 sounds and words:**
 https://www.flixxy.com/einstein-smart-parrot.htm?utm_source=4

- **For Da Kids #3: CGI Animated Short Film "The Box":**
 https://www.youtube.com/watch?v=20evunLzSgk

FOLLOW US ON: Twitter | LinkedIn | YouTube

Copyright □ 2014-2020 KnowBe4, Inc. All rights reserved.

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

Unsubscribe

Don't like to click? Email opt-out requests should be sent to opt-out@knowbe4.com

[Heads Up] How Slack Phishing Works - The Latest Tricky Attack Vector

To:	Adnan Memon (Sheriff)
Sent:	June 30, 2020 8:31:54 AM CDT
Received:	June 30, 2020 8:32:12 AM CDT

[Heads Up] How Slack Phishing Works - The Latest Tricky Attack Vector

From: CyberheistNews <donotreply@cyberheistnews.com>
To: jennifer.black@cookcountyil.gov, Jennifer Black (Sheriff) <Jennifer.Black@cookcountyil.gov>

Sent: June 30, 2020 8:32:01 AM CDT
Received: June 30, 2020 8:32:17 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

[Heads Up] How Slack Phishing Works - The Latest Tricky Attack Vector

Email not displaying? | View Knowbe4 Blog

Unsubscribe

CyberheistNews Vol 10 #27 | June 30th., 2020

[Heads Up] How Slack Phishing Works - The Latest Tricky Attack Vector

People need to be able to use their instincts in order to spot new phishing techniques, according to Ashley Graves, a Cloud Security Researcher at AT&T Alien Labs. On the CyberWire's Research Saturday podcast, Graves described a phishing technique that abuses webhooks in Slack to fool users into granting an attacker access to their Slack data.

A webhook is a feature that allows third-party apps to send messages to a specific Slack channel via a unique URL. Anyone can send a message to the Slack channel if they know this URL, so it's important that the URL be kept secret. If an attacker discovers a leaked webhook URL, they can craft a phishing message and send it directly into a Slack workspace to trick a user into installing a malicious app. This app can then exfiltrate data from the targeted workspace.

Graves emphasized that this attack doesn't have any visible warning signs, since the communication comes directly from Slack through a legitimate service.

"The only indication that exists would be the person's gut feeling that it doesn't seem right, that this app should not be requesting this level of data," she said.

Graves said part of the solution is improved awareness around what attackers can do with certain information. "So, I think some people legitimately don't understand how

much access an attacker can gain when credentials are leaked, and even more so when a webhook secret is leaked," Graves explained.

"On the other side of it is understanding what you're giving third parties access to. So, knowing to read those OAuth scopes, understanding how the application that you're using might use that access. Like, it wouldn't make sense – to me, at least – for a webhook to need access to my documents.

So, that's something that they have to look over and have some sort of understanding around whether it's some self-learning, whether it's included in security awareness training or something like that."

Graves noted that anyone can be fooled by social engineering, so companies need to ensure that users know when they should be cautious and ask for assistance before taking an action.

"But again, we've seen in similar attacks in the past that users can be easily tricked and that it's not stupidity," she said. "It's not even ignorance. It's just that this is very new technology to a lot of people, and the prompts are not always clear, and there is a lot of small text about how they work. So I think that companies need to, I suppose, make as much effort as possible to help people understand the impact of their actions."

Attackers will never stop coming up with new ways to dupe people into granting them access. New-school security awareness training can give your employees a healthy sense of suspicion to enable them to stop social engineering attacks.

The CyberWire has the story:
https://thecyberwire.com/podcasts/research-saturday/140/transcript

[Live Demo] Ridiculously Easy Security Awareness Training and Phishing

Old-school awareness training does not hack it anymore. Your email filters have an average 7-10% failure rate; you need a strong human firewall as your last line of defense.

Join us **Wednesday, July 8 @ 2:00 pm (ET),** for a live demonstration of how KnowBe4 introduces a new-school approach to Security Awareness Training and Simulated Phishing.

See how easy it is to train and phish your users:

- Train your users with access to the **world's largest library** of 1000+ pieces of awareness training content.
- Send fully automated **simulated phishing attacks,** including thousands of customizable templates with unlimited usage.
- **NEW! Brandable Content** feature gives you the option to add branded custom content to select training modules.
- **Assessments** allows you to find out where your users are in both **security knowledge** and **security culture** to help establish baseline security metrics you can improve over time.

- **Advanced Reporting** on 60+ key awareness training indicators.
- **Active Directory Integration** to easily upload user data, eliminating the need to manually manage user changes.

Find out how 33,000+ organizations have mobilized their end-users as their human firewall.

Date/Time: **Wednesday, July 8 @ 2:00 pm (ET)**

Save My Spot!

https://event.on24.com/wcc/r/2439681/925D004197E678DDCC946A93B31C24D9?partnerref=CHN2

[ALERT] A New Devilish Malware Worm Called Lucifer Is Targeting Your Windows Workstations

Palo Alto Networks' Unit 42 Security experts have identified a malware worm called Lucifer, that targets Windows systems with cryptojacking and distributed denial-of-service (DDoS) attacks.

This brand-new strain initially tries to infect PCs by bombarding them with a big list of known exploits, hoping to cash in on unpatched vulns. While patches for all these critical and high-severity bugs exist, the organizations infected by this new strain malware had not applied the patches.

"Lucifer is a new hybrid of cryptojacking and DDoS malware variant that leverages old vulnerabilities to spread and perform malicious activities on Windows platforms," Palo Alto said last Wednesday in a blog post. "Applying the updates and patches to the affected software are strongly advised."

The exploits Lucifer is using include Rejetto HTTP File Server (CVE-2014-6287), Oracle Weblogic (CVE-2017-10271), ThinkPHP RCE (CVE-2018-20062), Apache Struts (CVE-2017-9791), Laravel framework CVE-2019-9081), and Microsoft Windows (CVE-2017-0144, CVE-2017-0145, and CVE-2017-8464).

After a successful exploit, the strain connects to its command-and-control (C2) server and is able to execute any commands on the fully pwned device. Some "features" allow the malware to drop an XMRig miner and launch cryptojacking attacks, as well as collecting interface info and sending the miner status to the C2.

The malware is also capable of self-propagation with worm-like features.

The Threatpost site commented: "It scans for either open TCP ports (also known as port 1433) or open Remote Procedure Call (RPC) ports (also known as port 135). If either of these ports is open, the malware attempts to brute-force the login using a default administrator username and an embedded password list (a full list of the passwords used can be found on Unit 42's analysis). It then copies and runs the malware binary on the remote host upon successful authentication.

Please forward to your friends. Blog post with links continued here:

https://blog.knowbe4.com/heads-up-a-new-devilish-malware-worm-called-lucifer-is-targeting-your-windows-workstations

See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments and third-party vendor risk is a continuous problem.

We listened! KCM now has **Compliance, Risk, Policy and Vendor Risk Management** modules, transforming KCM into a full SaaS GRC platform!

Join us **Wednesday, July 8 @ 1:00 PM (ET),** for a 30-minute live product demonstration of KnowBe4's KCM GRC platform. See how you can simplify the challenges of managing your compliance requirements within your organization and across third-party vendors and ease your burden when it's time for risk assessments and audits.

- **NEW!** Demonstrate overall progress and health of your compliance and risk management initiatives with **custom reports.**
- **Vet, manage and monitor** your third-party vendors' security risk requirements.
- **Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.
- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **Wednesday, July 8 @ 1:00 PM (ET)**

Save My Spot!

https://event.on24.com/wcc/r/2439682/58CC9CFF88DA458F08828606604A4E42?partnerref=CHN2

Cyber Crime Uses Adobe and Samsung Servers to Hide Their Phishing Attacks

Researchers at Check Point have observed a phishing campaign that, to avoid detection, abused servers belonging to Adobe, Samsung, and the University of Oxford. The attackers used several layers of deception to disguise their phishing emails as legitimate.

The phishing emails purported to come from Microsoft and informed recipients that

they'd received a voicemail on their Office 365 account. If the user clicked the link in the email, they'd be redirected through a legitimate server before landing on a spoofed Office 365 login page designed to steal their credentials.

The redirection step was accomplished using an Adobe Campaign open redirect link belonging to Samsung Canada, meant for the company's email campaigns. Open redirects enable anyone to craft a URL that will route a user through the server hosting the URL before sending them on to the specified website.

In this case, the attackers used the open redirect link from Samsung's email campaign for Cyber Monday in 2018 and modified it to point to their phishing page.

"The technique of using Adobe Campaign open redirect was initially discovered in September 2019 on the domain belonging to Adobe itself," the researchers write. "In the last few months, it's been widely abused for phishing purposes. To evade detection, attackers abuse open and reputable Adobe Campaign servers to redirect potential victims to their own phishing websites.

This means that the link embedded in the phishing email is part of a trusted domain – one that unknowingly redirects victims to the phishing website."

The attackers also managed to abuse the University of Oxford's email servers to disguise the origin of the emails. "Using legitimate Oxford SMTP servers allowed the attackers to pass the reputation check for the sender domain," Check Point says. "In addition, there was no need to compromise actual email accounts to send phishing emails because they could generate as many email addresses as they wanted."

Finally, the phishing kit itself was hosted on a compromised WordPress site. It would generate a new directory for each visitor, as well as unique, obfuscated source code to avoid detection by security tools.

"The second layer of redirection is used to distance the final phishing page from the original email," the researchers explain. "In this case, the attackers used several compromised WordPress sites which contain malicious redirect code. Introducing another redirection layer enables the attackers to circumvent security solutions that investigate the links within the email.

Thus the URL within the email points to a WordPress site instead of a suspicious-looking phishing page." Attackers will never stop finding new ways to defeat security technologies. New-school security awareness training can give your organization an essential layer of defense by enabling your employees to recognize phishing emails that make it through your filters.

Check Point has the story:
https://research.checkpoint.com/2020/phishing-campaign-exploits-samsung-adobe-and-oxford-servers/

[On-Demand] 10 Incredible Ways You Can Be Hacked Through Email & How to Stop the Bad Guys

Email is still the #1 attack vector the bad guys use. A whopping 91% of cyberattacks start with a phishing email, but email hacking is much more than phishing and launching malware.

In this on-demand webinar Roger A. Grimes, KnowBe4's Data-Driven Defense Evangelist and security expert with over 30-years of experience, explores **10 ways hackers use social engineering to trick your users** into revealing sensitive data or enabling malicious code to run. Plus, he shares a **hacking demo by KnowBe4's Chief Hacking Officer Kevin Mitnick.**

Roger will teach you:

- How silent malware launches, remote password hash capture, and how rogue rules work
- Why rogue documents, establishing fake relationships and getting you to compromise your ethics are so effective
- Details behind clickjacking and web beacons
- Actionable steps on how to defend against them all

If all you were worried about were phishing attempts, think again!
https://info.knowbe4.com/webinar-10-ways-hacked-email

Let's stay safe out there.

Warm Regards,

Stu Sjouwerman
Founder and CEO
KnowBe4, Inc

PS: Just For YOU. We just added 2 new training modules featuring Roger Grimes about data-driven defense:
https://blog.knowbe4.com/new-training-modules-added-on-data-driven-defense

PSS: Need to educate your C-level execs? Here are five cybersecurity books that everyone should —and can— read, recommended by the Wall Street Journal:
https://www.wsj.com/articles/five-cybersecurity-books-that-everyone-shouldand-canread-11592579360

Quotes of the Week

"It is not because things are difficult that we do not dare,
it is because we do not dare that they are difficult."
- Lucius Annaeus Seneca, Philosopher, Statesman, Dramatist (5 BC - 65 AD)

"I am always doing that which I cannot do, in order that I may learn how to do it."

- Pablo Picasso, Artist (1881 - 1973)

Thanks for reading CyberheistNews
But if you want to unsubscribe, you can do that right here

You can read CyberheistNews online at our Blog
https://blog.knowbe4.com/cyberheistnews-vol-10-27-heads-up-how-slack-phishing-works-the-latest-tricky-attack-vector

Security News

Pyongyang's Phishing With Job Offers

An attack campaign with possible ties to North Korea's Lazarus Group targeted aerospace and military companies in Europe and the Middle East with spearphishing attacks late last year, according to researchers at ESET.

The campaign, which the researchers call "Operation In(ter)ception," used social engineering attacks on LinkedIn to trick employees into opening malware-laden documents.

"To initiate contact, they approached the targets with fictitious job offers using LinkedIn's messaging feature," the researchers write. "In order to appear credible, the attackers posed as representatives of well-known, existing companies in the aerospace and defense industry.

For each of the targeted companies we investigated, the attackers had created a separate fake LinkedIn account: one impersonating an HR manager from Collins Aerospace (formerly Rockwell Collins), a major US supplier of aerospace and defense products; the other posing as an HR representative of General Dynamics, another large US-based corporation with a similar focus. "

Interestingly, while the attackers' primary goal was espionage, ESET observed one case in which the attackers used a victim's email account in an attempt to conduct a business email compromise (BEC) scam. While BEC attacks are usually associated with criminals rather than state-sponsored groups, North Korean cyber actors often conduct financially motivated attacks to generate revenue for their heavily sanctioned regime.

"Among the victim's emails, the attackers found communication between the victim and a customer regarding an unresolved invoice," the

researchers explain. “They followed up the conversation and urged the customer to pay the invoice, however, to a different bank account than previously agreed, to which the customer responded with some inquiries.

As part of this ruse, the attackers registered an identical domain name to that of the compromised company, but on a different top-level domain, and used an email associated with this fake domain for further communication with the targeted customer.

The attackers did not respond to the customer’s inquiries and continued to urge them to pay. Instead of paying the invoice, however, the targeted customer reached out to the correct email address of the victim for assistance, thwarting the attackers’ attempt. The victim recognized something was amiss and reported the communication as an incident.”

Sometimes it’s espionage, and sometimes it’s fraud. Recognizing the motive can help recognize the attack. New-school security awareness training can provide your employees with the knowledge they need to thwart targeted social engineering attacks.

ESET has the story:
https://www.welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/

Survey Says...You've Been Pwned

Survey are enticing, and so are survey scams. But they’re easy to recognize if you know what to look for, according to Paul Ducklin at Naked Security.

Ducklin describes a typical survey scam that Sophos spotted recently. The scammers impersonate well-known brands and offer a reward to users that fill out a survey. Real companies use these surveys as well, but the rewards from a legitimate survey are very small, such as a coupon for your next order.

The fake survey asks generic, innocuous questions that could apply to any business, and allows the user to choose their answers from multiple-choice panels. Throughout this process, the site displays the text “38 visitors on this page,” and “6 rewards left” to induce a sense of urgency.

After completing the survey, the user is informed that they’ve actually won an expensive prize, such as a free iPhone.

At the final page, however, it’s revealed that the user will have to pay one

dollar as a delivery fee before they can receive their prize. To do this, they'll be asked to enter their name, address, and credit card information, which will be sent straight to the scammers.

Ducklin stresses that no matter how tempting the deal is, you should leave the site if you sense anything out of place. Even if you don't see any warning signs, the moment a site asks you to enter any sensitive information should be your cue to leave.

"Remember, if you are taking a survey and you see anything that doesn't add up – anything at all – then you need to get off the website right away before you get sucked into giving away any personal information," Ducklin writes.

"Legitimate companies and genuine surveys should be clearly explained in advance, so if the goalposts move halfway through, you're being scammed." Ducklin adds that common sense, awareness, and level-headedness is usually all that's needed to defeat these types of scams.

"There is no free iPhone," he says. "Or Android, or tablet, or laptop. There just isn't. Stores don't hand out $1000 mobile phones in return for you telling them whether you think they should stay open later. They just don't. Follow your head and not your heart."

New-school security awareness training can help your employees recognize social engineering tactics and avoid falling for scams.

Naked Security has the story:
https://nakedsecurity.sophos.com/2020/06/22/anatomy-of-a-survey-scam-how-innocent-questions-can-rip-you-off/

KnowBe4 Announcement: New Training Modules Added on Data-Driven Defense

We have exciting news to share! Two new modules have been released about data-driven defense, both featuring Data-Driven Evangelist Roger Grimes. Join Roger Grimes as he introduces the overall concepts of a risk-analyzed, data-driven computer defense, as conceptualized in his book, A Data-Driven Computer Defense: A Way to Improve Any Computer Defense.

These brand-new modules cover the following:

- An Introduction to Data-Driven Defense: Roger discusses the basic principles behind a data-driven defense and what most companies get wrong about cybersecurity risk and why.

- Data-Driven Defense: Hackers and Why They Hack: Roger discusses the different types of hackers and their motivations. If you're going to fight hackers, it's best if you understand why they hack and what they are after.

You are able to view both modules in the ModStore. Get no-charge access here:
https://blog.knowbe4.com/new-training-modules-added-on-data-driven-defense

The 10 Interesting News Items This Week

1. **This ransomware has learned a new trick: Scanning for point of sales devices:**
 https://www.zdnet.com/article/this-ransomware-has-learned-a-new-trick-scanning-for-point-of-sales-devices/

2. **Black Hat Survey: Breach Concerns Hit Record Levels Due to COVID-19:**
 https://www.darkreading.com/threat-intelligence/black-hat-survey-breach-concerns-hit-record-levels-due-to-covid-19/d/d-id/1338167

3. **Companies Name One of the Biggest Cybersecurity Threats: Their Employees - The Wall Street Journal:**
 https://www.wsj.com/articles/companies-name-one-of-the-biggest-cybersecurity-threats-their-employees-11592606115?

4. **Really good article on security awareness in SC Mag:**
 https://www.scmagazine.com/infosec-world-2020/lululemons-rex-sarabia-works-up-a-sweat-building-a-security-awareness-program-from-scratch/

5. **FBI warns K12 schools of ransomware attacks via RDP:**
 https://www.zdnet.com/article/fbi-warns-k12-schools-of-ransomware-attacks-via-rdp/

6. **Don't Fall Victim to These Common Social Networking Scams. By yours truly at Forbes:**
 https://www.forbes.com/sites/forbestechcouncil/2020/06/24/dont-fall-victim-to-these-common-social-networking-scams/#259d5d6e5462

7. **10 (more) free security tools worth a look via @csoonline:**
 https://www.csoonline.com/article/3563872/10-more-free-security-tools-worth-a-look.html

8. **Hackers abuse Samsung Canada, others, to launch phishing attacks:**
 https://research.checkpoint.com/2020/phishing-campaign-exploits-samsung-adobe-and-oxford-servers/

9. **Ransomware operators lurk on your network after their attack:**
 https://www.bleepingcomputer.com/news/security/ransomware-operators-lurk-on-your-network-after-their-attack/

10. **Ouch. BlueLeaks data dump exposes over 24 years of police records:**
 https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/

Cyberheist 'Fave' Links

This Week's Links We Like, Tips, Hints and Fun Stuff

- **Your Virtual Vacation this week: Eagle Creek Trail - Amazing Trip:**
 https://www.youtube.com/watch?v=T5DzGrDp5Xw

- **41 Next-Level Hotels To Visit Before You Die:**
 https://www.youtube.com/watch?v=FdkxZLfvm6Y

- **Ethiopia's Chapel in the Sky:**
 https://www.youtube.com/watch?v=IJCy64adY3Y

- **44 Things To Add To Your Thrill-Seeking Bucket List:**
 https://www.youtube.com/watch?v=0EPk5o_yvKY

- **How '1917' Was Filmed To Look Like One Shot. Incredible cinematography:**
 https://www.youtube.com/watch?v=kMBnvz-dEXw

- **Danny Macaskill: Mountain Biking Over The Ridge:**
 https://www.flixxy.com/danny-macaskill-mountain-biking-over-the-ridge.htm?utm_source=4

- **Pursuit - A 4K storm time-lapse film:**
 https://www.youtube.com/watch?v=oagszCmJLpU

- **Cats wake up their owner by cute actions:**
 https://www.youtube.com/watch?v=CL1Cdw_wtuk

- **The Golden Retriever Puppy Attack:**
 https://www.youtube.com/watch?v=Lc6db8qfZEw

- **Got a Pest Problem? Call the Quack Squad:**
 https://www.youtube.com/watch?v=H6Ehoxu9QY8

- **For Da Kids #1: How Parrots Express Their Affection:**
 https://www.flixxy.com/how-parrots-express-their-affection.htm?utm_source=4

- **For Da Kids #2: Einstein the African Grey Parrot showed off her vocabulary skills with a 200 sounds and words:**
 https://www.flixxy.com/einstein-smart-parrot.htm?utm_source=4

- **For Da Kids #3: CGI Animated Short Film "The Box":**
 https://www.youtube.com/watch?v=20evunLzSgk

FOLLOW US ON: Twitter | LinkedIn | YouTube

Copyright □ 2014-2020 KnowBe4, Inc. All rights reserved.

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

Unsubscribe

Don't like to click? Email opt-out requests should be sent to opt-out@knowbe4.com

Undeliverable: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	Microsoft Outlook <MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@cookcounty.onmicrosoft.com>
To:	CCSO.INTEL@cookcountyil.gov, Daniel.Moreci@cookcountyil.gov, Darren.Makowski@cookcountyil.gov, Dennis.Nicpan@cookcountyil.gov, James.Dillon@cookcountyil.gov, John.Hammond@cookcountyil.gov, Joseph.Giunta@cookcountyil.gov, Leonard.Jagielski@cookcountyil.gov, Miles.Cooperman@cookcountyil.gov, Patrick.Hecker@cookcountyil.gov, Richard.OBrien1@cookcountyil.gov, Richard.Young2@cookcountyil.gov, Joseph.Danzl@cookcountyil.gov, Zelda.Whittler@cookcountyil.gov
Sent:	June 30, 2020 8:40:36 AM CDT
Received:	June 30, 2020 8:40:37 AM CDT
Attachments:	Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

CCCASV02.CCOUNTY.com rejected your message to the following email addresses:

Daniel.Moreci@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins

The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

Darren.Makowski@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins

The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

Dennis.Nicpan@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

James.Dillon@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

John.Hammond@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

Joseph.Giunta@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

Leonard.Jagielski@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

Miles.Cooperman@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

Patrick.Hecker@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

Richard.OBrien1@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

Richard.Young2@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

Joseph.Danzl@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

Zelda.Whittler@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

Diagnostic information for administrators:

Generating server: DM6PR09MB5192.namprd09.prod.outlook.com

Daniel.Moreci@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

Darren.Makowski@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

Dennis.Nicpan@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

James.Dillon@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

John.Hammond@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

Joseph.Giunta@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

Leonard.Jagielski@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

Miles.Cooperman@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

Patrick.Hecker@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

Richard.OBrien1@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

Richard.Young2@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

Joseph.Danzl@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

Zelda.Whittler@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

Original message headers:

```
Received: from CY4PR09CA0013.namprd09.prod.outlook.com (2603:10b6:910:2::23)
 by DM6PR09MB5192.namprd09.prod.outlook.com (2603:10b6:5:273::18) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
```

2020 13:40:34 +0000
Received: from CY1GCC01FT004.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d02::209) by CY4PR09CA0013.outlook.office365.com
(2603:10b6:910:2::23) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend
Transport; Tue, 30 Jun 2020 13:40:33 +0000
Authentication-Results: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
CY1GCC01FT004.mail.protection.outlook.com (10.97.0.246) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:40:33 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:39:59 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:39:59 -0500
Received: from MWHPR09CA0043.namprd09.prod.outlook.com (2603:10b6:300:6d::29)
by BYAPR09MB3304.namprd09.prod.outlook.com (2603:10b6:a03:9e::33) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.25; Tue, 30 Jun
2020 13:39:56 +0000
Received: from DM2GCC01FT005.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::200) by MWHPR09CA0043.outlook.office365.com
(2603:10b6:300:6d::29) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
Transport; Tue, 30 Jun 2020 13:39:56 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT005.mail.protection.outlook.com (10.97.3.0) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:39:56 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
(10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:24:50 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:24:50 -0500
Received: from MWHPR09CA0042.namprd09.prod.outlook.com (2603:10b6:300:6d::28)
by BY5PR09MB4929.namprd09.prod.outlook.com (2603:10b6:a03:247::14) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20; Tue, 30 Jun
2020 13:24:48 +0000
Received: from DM2GCC01FT007.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::200) by MWHPR09CA0042.outlook.office365.com
(2603:10b6:300:6d::28) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend
Transport; Tue, 30 Jun 2020 13:24:48 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning

cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT007.mail.protection.outlook.com (10.97.3.159) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:24:47 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
(10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:09:37 -0500
Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:09:36 -0500
Received: from CY4PR09CA0094.namprd09.prod.outlook.com (2603:10b6:903:c7::32)
by DM6PR09MB5863.namprd09.prod.outlook.com (2603:10b6:5:271::7) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
2020 13:09:35 +0000
Received: from DM2GCC01FT007.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::207) by CY4PR09CA0094.outlook.office365.com
(2603:10b6:903:c7::32) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
Transport; Tue, 30 Jun 2020 13:09:34 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT007.mail.protection.outlook.com (10.97.3.159) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:09:34 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:08:33 -0500
Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:33 -0500
Received: from BL2PR09CA0040.namprd09.prod.outlook.com
(2a01:111:e400:c743::50) by MN2PR09MB5003.namprd09.prod.outlook.com
(2603:10b6:208:21a::7) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20; Tue, 30 Jun
2020 13:08:31 +0000
Received: from DM2GCC01FT005.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::205) by BL2PR09CA0040.outlook.office365.com
(2a01:111:e400:c743::50) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
Transport; Tue, 30 Jun 2020 13:08:31 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT005.mail.protection.outlook.com (10.97.3.0) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:31 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:08:27 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server

(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:27 -0500
Received: from BN6PR09CA0061.namprd09.prod.outlook.com (2603:10b6:404:7a::23)
by SA9PR09MB4784.namprd09.prod.outlook.com (2603:10b6:806:1c::21) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
2020 13:08:25 +0000
Received: from DM2GCC01FT010.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::203) by BN6PR09CA0061.outlook.office365.com
(2603:10b6:404:7a::23) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
Transport; Tue, 30 Jun 2020 13:08:25 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT010.mail.protection.outlook.com (10.97.3.132) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:25 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
(10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:07:52 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:07:52 -0500
Received: from BL0PR0901CA0029.namprd09.prod.outlook.com
(2603:10b6:208:1c0::39) by MW2PR0901MB3689.namprd09.prod.outlook.com
(2603:10b6:302:12::14) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.23; Tue, 30 Jun
2020 13:07:49 +0000
Received: from DM2GCC01FT006.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::203) by BL0PR0901CA0029.outlook.office365.com
(2603:10b6:208:1c0::39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
Transport; Tue, 30 Jun 2020 13:07:49 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT006.mail.protection.outlook.com (10.97.3.107) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:07:49 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:07:18 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:07:18 -0500
Received: from BN6PR09CA0049.namprd09.prod.outlook.com (2603:10b6:404:7a::11)
by SA9PR09MB5149.namprd09.prod.outlook.com (2603:10b6:806:45::14) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20; Tue, 30 Jun
2020 13:07:15 +0000
Received: from DM2GCC01FT010.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::201) by BN6PR09CA0049.outlook.office365.com
(2603:10b6:404:7a::11) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend

```
 Transport; Tue, 30 Jun 2020 13:07:15 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
 smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
 header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by
 DM2GCC01FT010.mail.protection.outlook.com (10.97.3.132) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:07:14 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
 (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
 2020 08:06:46 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
 by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:06:46 -0500
Received: from CH2PR09MB4491.namprd09.prod.outlook.com (2603:10b6:610:36::19)
 by CH2PR09MB4395.namprd09.prod.outlook.com (2603:10b6:610:6d::18) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
 2020 13:06:40 +0000
Received: from CH2PR09MB4491.namprd09.prod.outlook.com
 ([fe80::54b4:1a30:151b:810f]) by CH2PR09MB4491.namprd09.prod.outlook.com
 ([fe80::54b4:1a30:151b:810f%5]) with mapi id 15.20.3131.027; Tue, 30 Jun 2020
 13:06:40 +0000
From: "CCSO Intel (Sheriff)" <CCSO.INTEL@cookcountyil.gov>
Subject: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement
 Data
Thread-Topic: Pass Through - (U//FOUO) Criminal Hackers Target US Law
 Enforcement Data
Thread-Index: AdZOUZRVrVUDcfOlTiiWh3YE0iFXiAAjZyaa
Date: Tue, 30 Jun 2020 13:06:39 +0000
Message-ID:
<CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>
References: <LYRIS-103909956-1411846-2020.06.29-15.13.38--isp-les-
north#lists.illinois.gov@lists.illinois.gov>
In-Reply-To: <LYRIS-103909956-1411846-2020.06.29-15.13.38--isp-les-
north#lists.illinois.gov@lists.illinois.gov>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Authentication-Results-Original: cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=none action=none
 header.from=cookcountyil.gov;
x-originating-ip: [162.217.184.194]
x-ms-publictraffictype: Email
X-MS-Office365-Filtering-HT: Tenant
X-MS-Office365-Filtering-Correlation-Id: 2f90e5b8-3559-4ca4-557d-08d81cfb29b7
x-ms-traffictypediagnostic:
      CH2PR09MB4395:|SA9PR09MB5149:|MW2PR0901MB3689:|SA9PR09MB4784:|MN2PR09MB5003:|DM6P
R09MB5863:|BY5PR09MB4929:|BYAPR09MB3304:|DM6PR09MB5192:
x-ms-oob-tlc-oobclassifiers:
      OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original:
UrTnnB2hFcBuldWG/WlQW6SHaLsIud5b6OmyHpz6ITbVUSDZApWbWHRlBxrq5S5dDLfMQz21xkkKhXS5HG6afkS
OT0jNbfLp1jycbEoLeu3hfCPnml0/07xKsMLsD6S+idV/JjTXSEt2phgXXdGCuJSborJQvuHM330fsmL0dsFhyR
8BTnhjYpu9DwUkY2jeDxiuP/+Kcs2gfTgS5woIvA4kHUGZDLP1uCCotuOoepg85MUZui6PMlZZwjh4ZyU5rNJ9c
fBqeNVPc4TqSQNfhhiyaEI8NR55N59lIDhA+v8ZW3SldAtvxNvpYF5ffMVOK9FMwsJSxfEJfz8gmgh8f90QoVgt
0a+ZoW0X0FAONtg=
X-Forefront-Antispam-Report-Untrusted: CIP:255.255.255.255;CTRY:;LANG:en;SCL:-
1;SRV:;IPV:NLI;SFV:SKI;H:CH2PR09MB4491.namprd09.prod.outlook.com;PTR:;CAT:NONE;SFTY:;SF
S:;DIR:INB;SFP:;
```

x-ms-exchange-antispam-messagedata:
3y/sUpP1WvBTncjSe/KLUQQiBBzs5goYawJu81cTzjgwO1fgwzU1WPtWZoS4FoDDi3DMVAIdIdfpuokXWFzcBCl
JH/RRdNan1es6LJcm7EBQKKY8nTqup1BZ0QcHYn32VhgRDnfEfKkBJOnjiTBXFZgBLOdoIw2VXQy8Oco6WjWs+n
giN1EhXH2o98Mi+JBaiqQIK2x6FdAfOJw/H3I3sgfdVGVSh6EjUvOBOMY4U9dYWWMgHYlEUenZNbwXkSkV21i9m
+yQ6OeqyigRuUs7J7kDN+ndxJb/wU9mqRF3M8AtEAVqDvVKSOOPr5nSmZc0zgujltMclbvEaebrBq49Jsy1vrUD
7fHUY/G2yp24EPQ4V/wsCq5vlAMX7KTvyZfrOk6zFei12rAOoj4Hs+u+Whzr7lHXAsNeJOkhbdVT/7E+lMOHAzn
v2Ch3FlzZul/WN4MhDWeoXf/syfwzoWMnN5bckNXHOvxkITX8Mtagt/yWvCGWllA/quBeMFR8hdVd
x-ms-exchange-transport-forked: True
x-ms-exchange-transport-crosstenantheadersstamped: CH2PR09MB4395
x-organizationheaderspreserved: CH2PR09MB4395.namprd09.prod.outlook.com
x-crosspremisesheadersfiltered: CCCASV02.CCOUNTY.com
Content-Type: multipart/mixed;
	boundary="_004_CH2PR09MB44918DBCA1539E418B6FB17FF56F0CH2PR09MB4491namp_"
MIME-Version: 1.0
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
To: Undisclosed recipients:;
Return-Path: CCSO.INTEL@cookcountyil.gov
X-EOPAttributedMessage: 7
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT010.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(109986005)(21480400003)(166002)(356005)(19627405001)(52536014)(9686003)(26005)(550
16002)(33656002)(82310400002)(86362001)(83080400001)(81166007)(28085005)(186003)(347560
04)(7416002)(45080400002)(8936002)(8676002)(336012)(7696005)(6506007)(450100002)(833804
00001)(5660300002)(1096003);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 384457b9-30d9-490c-d838-08d81cf66e05
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?oUdt+OMUEgpHe7K1GgLl8CIhKhvdsZbi7/3etWxtJQwEHcja6v0LowhUj18n?=
 =?us-ascii?Q?lgJ4UHL89KtlCbeq5UhQ8y9fWQdds1Qf+Z+NYvq7O3Q6EOy4tojS4TkGAdpu?=
 =?us-ascii?Q?Pkro+hCzW+yf8ykeja3qMohGcxBkgYNpneaVmJpFyMoW0LiG/6NOH6M76mNQ?=
 =?us-ascii?Q?0REpj5ZZyqyfsrJbphJrvDm0Dph97GJIh8zrT7/3NQ1CwX5EnZqgPr431+xX?=
 =?us-ascii?Q?wYC7Ni4lg6BNAu5zmAvUFoI0at7N8ty8642sdtRJGkk6/VuHOOVdW4t82Eg6?=
 =?us-ascii?Q?5ERoF9MD8hNImjjMlOMsBBzcvTUqhCpyjBfJ6fdhtpGh1Af8RXv5RQnZ0tAj?=
 =?us-ascii?Q?wrgfCGN7e1jif/6nEjj6FLYr7cSoiiVHt+3JX6ncdlZu29I3US7TPropkhRX?=
 =?us-ascii?Q?gqcNmR2ZklJ2HWULNzaVXPg0ZEdkEcZObJba7NSrQRv978h0aAqNr4pC6Mow?=
 =?us-ascii?Q?uRb1deC8c0sMJAvmXIQPeAnM3fvT/vr40g42RVXf4Qa/99P589Ft1R81wRbb?=
 =?us-ascii?Q?DC/HgQVwaX00qvlOnUkyNpwhNvT9qo0ZpZ065fV8AL/x2nhd+eC8XAsnHXEi?=
 =?us-ascii?Q?9O4xWnVy2QqAgaiOKAf6bfANJxRuO2ElqwgbITWRPfYKR1Ggh/hEYtse85Ou?=
 =?us-ascii?Q?U7h4hKDr924vwZwc2tt6sXB55XJ91JvMX4Be3AlYavSFB03pAeYuoAQmZSVg?=
 =?us-ascii?Q?fw17uNqpLTCftV6SvtykHHQNBYk3T3Fd+DxvEMWQNLq/vB2DKXM9jzc63Ceo?=
 =?us-ascii?Q?8jfMxooNMX1llIgzNoV8LUqQao5n55R6Y3TIaEwYRbVkkdJW8eY/Of7voh75?=
 =?us-ascii?Q?Ad+bPJTV0AcbBJZiVc62b8LDMAugPMtcCVB4t8P402QZbEAG3lqiY/sAbTwZ?=
 =?us-ascii?Q?xerSjC1ZrYCX/fd9lo+DEorO/cIc45oMpSfbgQ2VJpwFj0IeJqzQbnPpPDxf?=
 =?us-ascii?Q?yIbCn7u8TIVj7tfpvDaeP3RmVuN7IWp9OxWwHlZtvRu3AsPVT20jIVuMhx5p?=
 =?us-ascii?Q?scnMjqLmzBSwO6AXk8aJDSh+WC7Oxh0LIncCy87LC1fAUIY6OrglbKMl4fbG?=
 =?us-ascii?Q?mzEZlNe/T6wPIWpdbsw5DKxMattBh4galhDuKTbOp8sptwGsHwSJIY50KhRg?=
 =?us-ascii?Q?sOLXCAJp5Gl35EpNfsfh+n/a4WATe4OKSYK6c23nxnQ3FKzJF3ejuVBtKDYe?=
 =?us-ascii?Q?yIFCAvg3qAzuYLTkWVXSOi3pw0gjFsAsewu8KQ=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: SA9PR09MB5149
X-OrganizationHeadersPreserved: SA9PR09MB5149.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT006.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(86362001)(33656002)(166002)(7696005)(55016002)(83380400001)(19627405001)(823104000
02)(26005)(6506007)(9686003)(109986005)(81166007)(83080400001)(5660300002)(8676002)(450
80400002)(8936002)(336012)(450100002)(7416002)(52536014)(21480400003)(1096003)(186003)(
28085005)(34756004);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 074aa61c-9bf6-4913-1757-08d81cf6823f
X-Microsoft-Antispam-Untrusted: BCL:0;

X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?OiPhxTPr1mzJ6BbC/3OsvKBfnl/N0/tduopiS5vJOz6wz4UyD7S00gSKZlUj?=
 =?us-ascii?Q?rhAKbzepbg8Yjf0r6ZcOcuBn/QoL/HVpxwIUdvTdBVWarfQjgPhoG4KhZVnZ?=
 =?us-ascii?Q?LnelQkUvsIeFmqvdoZ8iIuCW40RuwOmQufWuk5SYll3sx/o8htBZExO9hTE8?=
 =?us-ascii?Q?vPfwldkBMT3vrjQKNdcGiQWX4EtTb8ziLhgWgvfMli/Rcc7M2Cy7zIwPaK4v?=
 =?us-ascii?Q?2LnHjFhRcxBO74Nmne0C3Y0IU9d2WFO+g21QnMR1afCpSfgRwLlUEtIQnVIV?=
 =?us-ascii?Q?zUcHiexjKNv+OY85IY+cIo1NmWQ1JtC0qOsoXFvMuMNeCG3mqF827BO4GxTC?=
 =?us-ascii?Q?HrWbHgAU2DlEPKY+EXQz8Dy4w+9+4HVIdxDIjWC6w5iRhKwwctjej4+11zTb?=
 =?us-ascii?Q?99SVR9hyY20/rH7r2TRt1fXeFmZLbxPBUPxSKvzWVzIJzNs41IvD8TnFpscb?=
 =?us-ascii?Q?HNrHaOK2X99063AD5r0AbMM6RN36P7cHtufGppXwluURi6FYgZ7TIT5gRUVY?=
 =?us-ascii?Q?jEtu1SIWAHxxCuMq0LKwts0yXNJJQdQ4WvrHsx8OzfTdO7StBiTzML5rfm3A?=
 =?us-ascii?Q?VFxO+OJcEtMpg0r0u3j+d7t2WjjhRqj/ZnRfA/1B+1IphelbuKTof9S8M2Pc?=
 =?us-ascii?Q?b2rk8uD0NrpsuohEuJTUQ6bKnWACtzbqLUMWOU3STIYWNO9pj2PWhQO0UAhC?=
 =?us-ascii?Q?rm5BJSf7p6CFRZcXFipZZnxUsE1qMbuL09eGMC2LA33W5f/RV7SJUilHwekz?=
 =?us-ascii?Q?0M2/NAAFlW9uMwoQxVphCeGiVaVnPkpamb4PAY6F0sW8rg/SXSKm61Do5Hej?=
 =?us-ascii?Q?e6qqr87pQAsUTTuFAJNbicdE6ZwtvTv6W41G0XE6dJNCm7m8PrWy9aZsxLFg?=
 =?us-ascii?Q?8ssqzZ2YUX52HjR6D5YDUw43mpAePgvzaKYyg4PmyhwY1oaI61cfN2MRR5oA?=
 =?us-ascii?Q?6+9O9dv/CEIKD4p8ZsQL0ZMXraJkbTMam/7tMNw+YMCKgHI/JnULTuFxHBuI?=
 =?us-ascii?Q?UYn9z1U9cbRs0XWpOWeyXraXIC8e2nI3uc8TMwJUD0RdQTpkK/Q4ENE71P6J?=
 =?us-ascii?Q?ydYxxJB0zdiHmjO44EpGv0ywzp3Re/q5Tlv6aato2wz8lY7IzsOz6BUNbU4r?=
 =?us-ascii?Q?DItWO5VQ+SOZ1F9ejSZY6QbbJlods7kN7CaTX+w0dooYAfLLBEcMpEMxLTHB?=
 =?us-ascii?Q?m6PkFxzpcBStQG509PKjKGSWX5oLlW7TC7cgsQ=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: MW2PR0901MB3689
X-OrganizationHeadersPreserved: MW2PR0901MB3689.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT010.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(33656002)(55016002)(1096003)(7416002)(45080400002)(34756004)(8676002)(28085005)(26
005)(186003)(21480400003)(5660300002)(19627405001)(8936002)(356005)(86362001)(6506007)(
82310400002)(336012)(109986005)(7696005)(450100002)(9686003)(83080400001)(81166007)(833
80400001)(52536014)(166002);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 75d868a3-db35-4216-10aa-08d81cf696d0
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?9J2ei1fACgVRnX99cJQ4EA23d2ez5PpCeC4/xysLLYoK2n+170umL7WVDJR5?=
 =?us-ascii?Q?rlxODoxlp1ZygsRYfqb5bvLtl4d3935xgp+KmCt8rubV4wIl2Y/E43Tmb3bj?=
 =?us-ascii?Q?l1hAYtWDY4OI3Kg06dHfdJ7T4gqOshzX8d86bw0ThJlwpP19GapwYDRU0iJ/?=
 =?us-ascii?Q?dkUBZHuKsnaOuCb0GMteCgWCzxWyfESg4yPi1s0eGl4yWYistrFSoe4ko3Lp?=
 =?us-ascii?Q?NKe02PXTX61EC4jWNi3as07yGeBVDF+53tOrUl2/W+9TO5Gj4Cwq9z5m5YbD?=
 =?us-ascii?Q?NLYAnsnZoYI5mrgiB/tjx5ycxy8FnGwJJ8SLDRcOnZ2LIjfbFjJsJlA6z8//?=
 =?us-ascii?Q?DaJVVqbuHAw26KpYVnonodRPJmhk3Yknby0JZNL5cx5Tu+zB1PKf7+P/Q9gS?=
 =?us-ascii?Q?WLQJ0/sjcMxYb1j/hgbg2iXsY/4bAxDaqlIXX17p/Rfjm9YVth8QSdcXKkOV?=
 =?us-ascii?Q?qPOsurUPqUIy0XrUh44olBTSkTGIe4orz2ln6hlukdT4PqakRtgxwyE3QO59?=
 =?us-ascii?Q?iBBmQi0LK0rURzzENQjgtfmLv8QDNa3XKPfQaX+bkkcYUpFpVoU2enQYGrk5?=
 =?us-ascii?Q?84D44TppipB9Tluyed4p3Md5os8q+UpCy1nCrlJuqHXtzjV2/l8qV8ApQnp9?=
 =?us-ascii?Q?0UpyaZ9fYsCNB9NncJ4oX3D33YtI/GIcKJoQqq4N222/ipk9ZV+5FBl30u6x?=
 =?us-ascii?Q?qlrdvikighUXmAPnkqDpMoOUZJIblpAzOOXc/23qIxNhY7HauetDVMPaL228?=
 =?us-ascii?Q?OMLa0kExuPYpfKrOFvE7Q9gctwrX4+BiPTTFgbpOAxS1KE0Tlgz/sglSvj0r?=
 =?us-ascii?Q?wPHU++CaYxE4iyrRfrQ8T2Y6Nw8gogF3I8V9POlR4iFn630bziuWyg7bcbw3?=
 =?us-ascii?Q?6RiaIrxERmO6yLzjzsaC8RADW5Ii8/10dOHVPxFXmBCgcEDdSMse3X1PEjEV?=
 =?us-ascii?Q?7K98OOxunyhmFA3MrDMpcFVyfDdvSBFnsy0NKPy6yQa23Zkx7N5YcRR/XrEY?=
 =?us-ascii?Q?YrKci8mMdkLPYdOuCT6dzmYSZ9B4AtPvFkLy7gWLpPJMjTMYxCbJQIKSs+j2?=
 =?us-ascii?Q?Rhkm5i30KB0VeKWrSaQfF/5CYLwuKVwKDqObvhwpO3WcIWI3wTtJpVzdF/+A?=
 =?us-ascii?Q?Ou1z+AGBqDZkRQN8/PEzxR87do4hCeQ3C6OtOGaeoLjLSw+hQFBs5T1nBZuV?=
 =?us-ascii?Q?y10XNBQo3enwxhkRze+doWFXxBOyNplW19hVwg=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: SA9PR09MB4784
X-OrganizationHeadersPreserved: SA9PR09MB4784.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT005.eop-
gcc01.prod.protection.outlook.com

X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;SFS:(166002)(28085005)(81166007)(336012)(83080400001)(19627405001)(45080400002)(56603000002)(86362001)(21480400003)(52536014)(33656002)(6506007)(450100002)(26005)(186003)(83380400001)(34756004)(9686003)(8676002)(82310400002)(7416002)(8936002)(55016002)(7696005)(1096003)(109986005);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: fba07594-0eee-48c2-8215-08d81cf6ac44
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-ascii?Q?U6/abOYHvFUbfdPEmducHBvNxnh8Kj0PZNteupvrpqeTxo2fjmYLVmMwZgwY?=
 =?us-ascii?Q?OWEW7no7FVh5kaGKvLe/+fYTedVjjz3PE/UxV1fUAYBq151b+C1wG08dy5jB?=
 =?us-ascii?Q?WCDhqRf4+238KaEu+wq2fykXFP0MuM4wFYKvqkIo8JDK1AArYvbMUnYqFk3z?=
 =?us-ascii?Q?qPKRNviv1WxjTh7ubNwGi2VLbnje7vNNbSthVpVwu4Tmmk6MWOrF9+11n1Sp?=
 =?us-ascii?Q?ZxfQWM++uisbi6m1Q2se+dgYXg7bLySv64bOJHW4C7kqDdJOjjD6lPB4ScIc?=
 =?us-ascii?Q?qmPJr3GPrdmfJPx9OaSYcYRExzM6WrKRTGSc5dgjU+1FbEkgtkafS4CZaAXr?=
 =?us-ascii?Q?KKttEXpEBE/ThZbZGGuNPQmT+g0/j9vr56zEMpSWkVrkTk8KFT1/dT3iZTHI?=
 =?us-ascii?Q?J8pAi/C/XXf7abHLt5uMECDrdKg2APepydHAVuuFTb2+brZrBd7hwyFC3x6A?=
 =?us-ascii?Q?wfCP0IGSXGXN67BzstdQBw42+FODvoA43lDMJ5cMSBrAohLr5ildyMCXqKWU?=
 =?us-ascii?Q?3u4DqDostvPvOu5tpt82wLYg1P5Dbjncq4WIXp8CsBwJsIJ1LAJNzfXYMhle?=
 =?us-ascii?Q?DVCqb/BrBQPF+hWwkacCFHcwP8x0WpHhLUCi3+GSIr0polQKkzF2GAT1qiho?=
 =?us-ascii?Q?CRw+rjPIM/G8CzwQICiIDkibj9I+VCyIw21ToT3kNRLYjb2SUcJTe3mBoxYa?=
 =?us-ascii?Q?DC0Waa7DaAgEi4Q6jabFTa1OiSl5/MjsrZlK3CofvmjdO7XaUZl2mxKsJjwL?=
 =?us-ascii?Q?aMIwdXVXQT3ucSZv8ug/rLwgcQ2NqvmFLlBgjj7OsKDypRt6mQ7G+5X8aTmA?=
 =?us-ascii?Q?7898+Ld/Zr/kuxs4JWR10iwX1BOeC8SLWPPe+Ps0TZfmwtAcqNh5E9mdyCU5?=
 =?us-ascii?Q?qL0lIWorJWuYsDT5GqswjsTekEi+FE9GxP/FH3fnY8KmX1woesP3Ssfvb775?=
 =?us-ascii?Q?uGiJv6B/km73Fr6wLxjYLf2yC0AkbrWd9io7U/xeD4+ToMmNa9PyBocOAYPW?=
 =?us-ascii?Q?kcGEN7eZwaEGtbXPwE7/08hPOfzdUhAhqPiE0RH3rbLVh8gMRRLDlnZZhxYA?=
 =?us-ascii?Q?bnCqtYeLC1V/Q7xfJFy0u4kmlCg1n6KOvSFrtUncW8z16kR85t+4OK69uuLG?=
 =?us-ascii?Q?Df1i58328Pa8ufDEkB25wHZvjbMEHVBUkSfYv27dRleO3RJecqfkPopAjtpy?=
 =?us-ascii?Q?15jBU0Fn9YiNjaIJRuX0/dmxTsmKknIEElNsTQ=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: MN2PR09MB5003
X-OrganizationHeadersPreserved: MN2PR09MB5003.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT007.eop-gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;SFS:(82310400002)(9686003)(450100002)(21480400003)(83080400001)(7416002)(55016002)(6506007)(5660300002)(45080400002)(83380400001)(52536014)(33656002)(109986005)(336012)(1096003)(28085005)(81166007)(34756004)(26005)(166002)(7696005)(186003)(8676002)(8936002)(19627405001)(86362001);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: e1bc1680-6c08-415c-1f4f-08d81cf6afee
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-ascii?Q?ztxSBFV52yZ/j/LUyA0/2sKYbqvSuSKr4anXyJqGAezpsh7g7FreGXxsU21r?=
 =?us-ascii?Q?PxmlSV1cwMvBuM0KKbRXr5pw1VBPMkSV6WR91AeFKdq4vFPqYH+KNKmy8Tqc?=
 =?us-ascii?Q?tJqD2ZNiKWOCW4KtGdZqSMvT+m9mONftE14x4kNwQWv97N/gD7h4rhc2YkZ4?=
 =?us-ascii?Q?R2FbhlZTGHCZyqu3R48Z1ighLCUkcl1T7vLdNfIaxOgrSCeHsMwHpY95xxhg?=
 =?us-ascii?Q?bZMrB3tGMmFIxY3XMDSkLdI+EaSFI54vjSXv1+IW5zjc/K1WnYCVU2Hv7+jT?=
 =?us-ascii?Q?9R4DlOWkdnXDZrcPktKZ08zoKsGC669zbVh666yP6saHF+FCwIBdwea+scdt?=
 =?us-ascii?Q?41v4Hnaptb1HqYl9+ayEUZ97jKO6nxGftv9Nxfc8lY6h4AmzzKgE3kpsSma/?=
 =?us-ascii?Q?yW39G1wtOrCZTafst4Fw/dDfUS5AbNj1q//x2Ff7V7meuMQs6gchTOZGYAf6?=
 =?us-ascii?Q?o1b1uBRn11rwGpusTsX0Ah3SDh5kYczJOiXOef9V1dVk+VMFrAVYjQ7q2nOz?=
 =?us-ascii?Q?itGKtURd6BcsFwcZyaVUS8R3E/J+HVGwBJYLFb+Lifd0NkNTa+EuPUbdJf1z?=
 =?us-ascii?Q?/KaCWvh2ecTJpUJLkjGtxA6cvxOyxnrcM1PZnEPy6NyqS889bpng07Ong/rq?=
 =?us-ascii?Q?cF16jysmYaEJg0s/XzwtIg7DBsitye7vc6MD6rzuEt0QWgpvn7Q+NuFUzU5v?=
 =?us-ascii?Q?UV6tl4UVimIm9jIyfifcUchhQa2n649PNBfefhL80qiAWnTNqW+xj8vLp/BD?=
 =?us-ascii?Q?qbx3+2NixIC5RMpXDewXLizY5DSyUes42lRmCWQAhjsuNmoYqi7ILmSuazM7?=
 =?us-ascii?Q?W0C6WUwQwI8vdzt0SNOKAbvfkSsMZ7kR0wt3hR2/0u1CkmElidinzrsZccJE?=
 =?us-ascii?Q?wolcYXfW3BoTFS4m25ZH53TymLdGEhqK2Cihvz8kvFEjMEB2rGqbADYuBgL/?=
 =?us-ascii?Q?RzoNxko4GXNcClcAbibEgRVVGnfTiOK4/yGAOnvsVVIIWxCYhAKHmu6KOzS9?=
 =?us-ascii?Q?o95BPRNBjxqef8diGnvCvd6i4xWQg7ywyrLfqWC1E9kMaj8Z6XIo/UCpypJE?=
 =?us-ascii?Q?s5iXHCeizpzrwOazYUk8c/8RL4EknOl/3aWwfBI4Cqw2cYOYwVaInvjLZyjL?=
 =?us-ascii?Q?pdR7nzmpe622VxhztmwXmxbT1TXfCTCXeu/qw2CJAw6/k/NQtG53XpL5HXN9?=
 =?us-ascii?Q?nssil8iXy5adU9LHz/OtbKtt683yWQ4ieQpS/Q=3D=3D?=

X-MS-Exchange-Transport-CrossTenantHeadersStamped: DM6PR09MB5863
X-OrganizationHeadersPreserved: DM6PR09MB5863.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT007.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(33656002)(55016002)(21480400003)(336012)(86362001)(5660300002)(8676002)(8338040000
1)(52536014)(45080400002)(186003)(7416002)(450100002)(19627405001)(28085005)(34756004)(
9686003)(166002)(6506007)(356005)(109986005)(26005)(81166007)(83080400001)(7696005)(893
6002)(1096003)(82310400002);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: f3d4eb42-e293-453e-7376-08d81cf6d59e
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?2iQuMMGnrUWx6ax2DTAny/OLk5uakci1+V4Sf8YzceiLryYKsHXfotMV0TYZ?=
 =?us-ascii?Q?NfI+K453cbAUo7paLbsHbl/hNsYXqKgGuHKnRc0RaYTgBwNIdxQs/Y2OV2dj?=
 =?us-ascii?Q?bHG1Vpwwjhl4CaDjNmRPryvcKaJ/yN1GwP2YywJEc9DIrl3J0Vn7saHA7pjX?=
 =?us-ascii?Q?iTk5ho+zwVubK8eCQcib6GWAq3RM9f5ApkKxnLHZ1oN9Mh6kybm9NOQClHLZ?=
 =?us-ascii?Q?GIQSrqKKIrxGXvfDAQmxyQr2I3i5heQE+EWZfq8YogTze0JvthNI+/9Y/uoK?=
 =?us-ascii?Q?uGjc4/WMdqOz32AbtLkBnhWv1sTHbxhH1ZguxBkj9bzKaR7RZnmGYxsSS9dN?=
 =?us-ascii?Q?x2/HcS3Es/qLXx52KVHSdS74tRPChQ18bQJtSicwdWovr/OaA9A79tINqcix?=
 =?us-ascii?Q?Zhbj+OWn/b5RrPRME+SCOkq1efuGoJLBV6KfT1H4OxFFU+L7UyUh7FTo3UoN?=
 =?us-ascii?Q?5LZ4KQyB6Lqlhjm8hwPYoaWJ0KHitcBDeYMef7QF8G2BX4SwUPgwT0L4hk4U?=
 =?us-ascii?Q?yueEOwTICaazHUOuv39pYfmGuefQ1E0zSDBKRhNAECJyDHZWpDogXsK6kYWU?=
 =?us-ascii?Q?825SAzVmNoGNs5J6YY3WtkYV+4CWzLO7UcyjHvhHz9GI8iEcJhz5dx+W5FQY?=
 =?us-ascii?Q?B6AmRVa/HdrL2OWSci2HgeubEXqS6CURAhucGiOEf2aiTEtz40aDHsAP92M5?=
 =?us-ascii?Q?sF6wiEhYB5EDdCwfxD5H7cSfQ2SVLSexd4FcL9Qlfi0LjvyrH35z+uhAMUJy?=
 =?us-ascii?Q?69Mjg8cIFLUxcmmwa9suXMAoIZXlCf9YGQDpceCVtGnigPlk3vEhHkraN8FD?=
 =?us-ascii?Q?mUNJCn+1gubP4eMj1e106Vv3T1rnd3xqLwtVl3Nx/2GFE8qf/pgiFl1u9Ryr?=
 =?us-ascii?Q?+QkGj47yF9KYJZlDRkJjD3cnsQiT3hVNRoZreRaM3pMjPai7BwsL8CzA+2Xy?=
 =?us-ascii?Q?GpDpg4VVRR3NOPCCQFaE/9kOU37eQ08ClpWHhPjQK1TAoHulQRZMT8aLrR56?=
 =?us-ascii?Q?ufwP0A6LgZGeYmcWOwmlNE7w4ijnAAuU41ppLxoouobVrVL/0mdmSta0MvTD?=
 =?us-ascii?Q?rLWflFroFDVX16SGmBfOZQixR9vDt90/ecuNlFNC4mVD0w1AB/tvQLFFWIyN?=
 =?us-ascii?Q?wwwQDqubPiJkUkh+JMxxYHh1RXkWCEh/fmZrYyiHkk/gn6PeKFv/Y11uotlL?=
 =?us-ascii?Q?6vWfAZWgsND9RTlf6ek8k+3E1aEcw6b8k54a6Q=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: BY5PR09MB4929
X-OrganizationHeadersPreserved: BY5PR09MB4929.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT005.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(83080400001)(109986005)(82310400002)(356005)(7696005)(8676002)(166002)(19627405001
)(21480400003)(83380400001)(81166007)(1096003)(8936002)(9686003)(28085005)(450100002)(4
5080400002)(34756004)(86362001)(7416002)(33656002)(52536014)(186003)(55016002)(6506007)
(5660300002)(26005)(336012);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 5ed7fee9-80c1-4310-9a19-08d81cf8f62b
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?DuNLeHlGGVjPNKsYCtFRq1cuHFwsd3Byk8iwd6UxmE7ZEdJBz/yak1CBwoln?=
 =?us-ascii?Q?4us5OxbjY4NwPOIxvQUrWSCBZGiU+ZhVNY1mJd9aOaWOZgdakMPTY6S6FR49?=
 =?us-ascii?Q?xHw0fs/pTD5EwMJDdP91MesF7iwUYuLj8FgYOgUMQMIH5vd1DYkw7q7JNFf8?=
 =?us-ascii?Q?naGDquZGor0xPUNjv+y7SfbKr0JXcfqF1/LW4fYkxqVsuYLwaUdfCLtY9XS5?=
 =?us-ascii?Q?mTl+yBJP8lJgrd7EadTfUNpxTbNJkX23HkMhjJX/XBXs11Wt/VFqmWHPN917?=
 =?us-ascii?Q?ziMEcwmjQvFJ23k1QWvDkPugxzN6Il4GLFl4LeUdtZCdn46EB7S1VL77xSCU?=
 =?us-ascii?Q?E9l/FD6Fs7L34aX1z94G1zUEz5rHd7ppwSSaTrDFttiixadzMXIQBqXRL0Gz?=
 =?us-ascii?Q?8mRsCdsmbZz5FDSEAGkx7KUyUAxTVv1zL1LLS501ybZHm8WSc3+EuM7W+rC6?=
 =?us-ascii?Q?JfEvaf1zzYkBgrqnT/7pXzRoLrSGgDUV3d2fx499cvALvk6Fmd58QmXSJ8iJ?=
 =?us-ascii?Q?rryLw8mVjbkWnGNVfFN/jfqtdJBHJluLSCFLaVDss0ruEJdw0TV/eUzfx7aN?=
 =?us-ascii?Q?whV7+VHUrfUS+ncVdnYQnAnVpFLqt8yWb73XBTxRywNFlmOjitldH9EGoFZ7?=
 =?us-ascii?Q?pBpsVqtdvjtZI6QyHYZPomtfG8Ej82h/+f0FJ0JzcQQgXYNb+PJ3B6C0vfGs?=
 =?us-ascii?Q?v01TaHo7b0VqL4t3eZimGmkOh/ecURHtCIwnH1lhih1Q3vBvnTi5KvodG0lO?=
 =?us-ascii?Q?9UF4XP8AQtUuda6zAdAPQJ2DhZAeh1uQQtD5UpsEmzIlJDUhaC9nyPCjtd58?=

```
 =?us-ascii?Q?Gz9u0PAelS/PytyhcgzIeOhvlPTLW/8moDoxPH2HwwgCx6j7aAGzLnGuZONd?=
 =?us-ascii?Q?HvS+4ZmaaZXQjMSx+UEbdTy4TFuykybC4c7LOnPswlmD8yBXMKOJbWbVL8HB?=
 =?us-ascii?Q?ofIxCE3tTtR+kulsTNZVV7Hhc70tv1BZvNHFHT9JqiV5rXWdHfSx+Pq62kpl?=
 =?us-ascii?Q?4+ltOeFKkcZ+nxjIwoohpvPJRMuGUzblXi9tLp6ZFcWgT0pesBz42H69s2dV?=
 =?us-ascii?Q?U+nkPw2ONzaqFrMe/Fk5z/+JX67fAQKq0IXTZ6o+RYswZN9zP+kAL/uxGv08?=
 =?us-ascii?Q?RWMHFXcyaGOw39byC3iVzcI8RjU29FLyZVJPkmi+6j2vURLvKH8YL+0CrG4/?=
 =?us-ascii?Q?BI8ipxxBetU8g4xdQCibE+epInBFegamECRecg=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: BYAPR09MB3304
X-OrganizationHeadersPreserved: BYAPR09MB3304.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: CY1GCC01FT004.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report:
      CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(6506007)(109986005)(7416002)(186003)(19627405001)(82310400002)(8676002)(450100002)
(1096003)(8936002)(7696005)(26005)(336012)(34756004)(55016002)(45080400002)(52536014)(2
1480400003)(28085005)(86362001)(166002)(83380400001)(83080400001)(9686003)(5660300002)(
33656002)(81166007);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs:
      1ccef75d-1188-4b00-6fcf-08d81cfb1387
X-Microsoft-Antispam: BCL:0;
X-Microsoft-Antispam-Message-Info:
      =?us-ascii?Q?rY4asHruCvlB8MPnw1Q2K3Fp5mywOGMdYccK8gW+5DUWNELxWxLFVcwFEjOM?=
 =?us-ascii?Q?R8hmD0gVu5QRODbV3240rPcgEO1mkcJ60QL7GftBTZYQEfoPCgbKzJOMH64E?=
 =?us-ascii?Q?5gdgcoJtulq6DMTiQ7MoTfvPtsnP6yGi8vgvtDQxMu4avnUosLKP7iAPwH79?=
 =?us-ascii?Q?94CtPxpI2DEuvGT94GNYZh/+0IYhGOcd9r/Jv65KYMLNdWNyepF4yRiA/N/a?=
 =?us-ascii?Q?DzCrRn5dAjGy8coSPF9r0Zjor98X+2ENksm3p0htt4Ia8mFP7jQdDDi+Iv+6?=
 =?us-ascii?Q?uXEFW8zuWc+GUoG1dv7Dan9EOUBjOhfKvkQIIM+PFNLhu1cXrodrRV1hJwKO?=
 =?us-ascii?Q?JiKF84q8R6MqfNIZEbwZ9bwXVZz+kqwp6Xv3Ui+X2vmuG/FWUO+N7M/Qt+tz?=
 =?us-ascii?Q?cI/52nxGI29JcppJce2H0NTe7Ic8mu171rZkP24RWbQyJmr4PWcMYTnBwSsa?=
 =?us-ascii?Q?XZsp81qSctaZPexij0wBRYpvnK3sUcsoVSqbdxdH1TGBLreUAyvxQEErHckw?=
 =?us-ascii?Q?zR2ASchZwY19a1w6j6FY93/t706iFJ08+lwt+vCmIdmUAJKdeIL88kxicJlx?=
 =?us-ascii?Q?eM/+Kgbz+UmDITg8o6BLRYvYYCYjUmUYSPaKfJXUhHoIE3tsLPg62ugCE0Yq?=
 =?us-ascii?Q?+wfqUjnoWUVJbdB3jM30pLNgC4zCzaJEvXJ0hVjZ1Aw5rqOwdq+9INa4/+wK?=
 =?us-ascii?Q?EGvk4cbSIcCWKPdJUvIffgj64fQzKM+KJ2ipKESw0jf03ej4DnTAeQSGrk7l?=
 =?us-ascii?Q?o69icAU0gD/FKR2Sl8slDNQ3udqSst8GCf+SI/iUtxmGHLxuFRIMt0PNKbcw?=
 =?us-ascii?Q?tDCW20zGtZ4i+Vkvp36/CW/eWCsmX6OdWSWG3PZx8NddTbNizXvW/ncgSbBy?=
 =?us-ascii?Q?HPhbD20L4fVU4s+vwRoRTlAcdZwvPGHOz9HMFjgT4NZ11CspTtCXMq3sjSpy?=
 =?us-ascii?Q?lTau1wz2G9OwbcafVj4XQjzEHfbZ4qzptkC6ZFplp1SI+1yAQC681+PtjeMu?=
 =?us-ascii?Q?/5ePGDEX89hMBJiKP9vauks57IzHAUCxhtoqCLvp+Assx8mcbWHcaaX83c5o?=
 =?us-ascii?Q?Wvh+pXW5DBwiXUzU2xhRBx4faZH5SQPAnVG35RIqs1CNJZq4hgrahqrN6Zxx?=
 =?us-ascii?Q?8vpVsSepJrT6fNikXSTwdIF3tJ8Tz0xKooKOWy6CrfSloj90SzuYRPRosmFO?=
 =?us-ascii?Q?t3/uIDh8oAiNQN53dGpxQXkGNYEXevD5fLhML3Ob9te8uk4vd/Ipmlg95EjD?=
 =?us-ascii?Q?SLGpjMMLKJGGWhSEnQZm?=
X-OriginatorOrg: cookcountyil.gov
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 30 Jun 2020 13:40:33.4265
 (UTC)
X-MS-Exchange-CrossTenant-Network-Message-Id: 2f90e5b8-3559-4ca4-557d-08d81cfb29b7
X-MS-Exchange-CrossTenant-Id: 8b4d55ae-6db4-4e05-a85c-59d6a256cd6e
X-MS-Exchange-CrossTenant-OriginalAttributedTenantConnectingIp: TenantId=8b4d55ae-6db4-
4e05-a85c-59d6a256cd6e;Ip=[162.217.184.79];Helo=[CCCASV01.CCOUNTY.com]
X-MS-Exchange-CrossTenant-AuthSource:
      CY1GCC01FT004.eop-gcc01.prod.protection.outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Anonymous
X-MS-Exchange-CrossTenant-FromEntityHeader: HybridOnPrem
X-MS-Exchange-Transport-CrossTenantHeadersStamped: DM6PR09MB5192
X-OrganizationHeadersPreserved: DM6PR09MB5192.namprd09.prod.outlook.com
X-CrossPremisesHeadersFilteredByDsnGenerator:
      DM6PR09MB5192.namprd09.prod.outlook.com
```

Undeliverable: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Daniel.Moreci@cookcountyil.gov, Darren.Makowski@cookcountyil.gov, Dennis.Nicpan@cookcountyil.gov, James.Dillon@cookcountyil.gov, John.Hammond@cookcountyil.gov, Joseph.Giunta@cookcountyil.gov, Leonard.Jagielski@cookcountyil.gov, Miles.Cooperman@cookcountyil.gov, Patrick.Hecker@cookcountyil.gov, Richard.OBrien1@cookcountyil.gov, Richard.Young2@cookcountyil.gov, Joseph.Danzl@cookcountyil.gov, Zelda.Whittler@cookcountyil.gov, Ricardo.Hardy@cookcountyil.gov, Wanda.Walker@cookcountyil.gov, William.Mak@cookcountyil.gov, Alexander.Brodie@cookcountyil.gov, Lisa.Farinella@cookcountyil.gov, Kevin.Graff@cookcountyil.gov, Kevin.Cooper@cookcountyil.gov, Kevin.Christofidis@cookcountyil.gov, Kelly.Sweeney@cookcountyil.gov, Jonathan.Mobley@cookcountyil.gov, John.Steed@cookcountyil.gov, John.Pradun@cookcountyil.gov, Jeffrey.Pasqua@cookcountyil.gov, James.Scannell@cookcountyil.gov, James.Hughes@cookcountyil.gov, Lissette.Rivera@cookcountyil.gov, Giovanni.Veitkus@cookcountyil.gov, Gary.Newsom@cookcountyil.gov, Frank.Caridei@cookcountyil.gov, Felix.Arvelo@cookcountyil.gov, Diane.Haras@cookcountyil.gov, David.Delgado1@cookcountyil.gov, Daniel.Strong@cookcountyil.gov, Daniel.Burke@cookcountyil.gov, Cedric.Mccloud@cookcountyil.gov, Catherine.Domine@cookcountyil.gov, Anthony.Burns@cookcountyil.gov, Gary.Rizzo@cookcountyil.gov, Luis.Santoyo@cookcountyil.gov, Mary.Tamme@cookcountyil.gov, Wanda.Barnes@cookcountyil.gov, Vincent.Gamez@cookcountyil.gov, Thomas.Shader@cookcountyil.gov, Tangenise.Porter@cookcountyil.gov, Tamara.Levickas@cookcountyil.gov, Samuel.Cory@cookcountyil.gov, Ronald.Prohaska@cookcountyil.gov, Roger.Comer@cookcountyil.gov, Robert.Waller@cookcountyil.gov, Robert.O'Neill@cookcountyil.gov, Richard.Petersen@cookcountyil.gov, Rex.Knaperek@cookcountyil.gov, Paul.Riley@cookcountyil.gov, Paul.Huss@cookcountyil.gov, Nancy.Pavelka@cookcountyil.gov, Michael.Quan@cookcountyil.gov, Michael.Gomez@cookcountyil.gov, Michael.Anton@cookcountyil.gov, Maurice.Cernick@cookcountyil.gov, Matthew.Walsh@cookcountyil.gov, Eric.Sellers@cookcountyil.gov
Sent:	June 30, 2020 8:40:36 AM CDT
Received:	June 30, 2020 8:40:38 AM CDT

Undeliverable: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	Microsoft Outlook <MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@cookcounty.onmicrosoft.com>
To:	CCSO.INTEL@cookcountyil.gov, Ricardo.Hardy@cookcountyil.gov, Wanda.Walker@cookcountyil.gov, William.Mak@cookcountyil.gov
Sent:	June 30, 2020 8:55:34 AM CDT
Received:	June 30, 2020 8:55:35 AM CDT
Attachments:	Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

CCCASV02.CCOUNTY.com rejected your message to the following email addresses:

Ricardo.Hardy@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44919AB3DDCF48A1DC9A721BF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

Wanda.Walker@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue. Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44919AB3DDCF48A1DC9A721BF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

William.Mak@cookcountyil.gov
Something went wrong and your message couldn't be delivered. This could be a temporary issue.

Try resending the message in a few minutes. If that doesn't work, forward this message to your email admin.

For Email Admins
The message couldn't be delivered because a mail routing loop was encountered. This may be due to a routing misconfiguration in the mail flow settings for either your organization or the recipient organization. If mail flow settings were recently updated, this error may be temporary.

Check the message headers in the section below to determine where the loop may be occurring and if it's something you or the email admin for the recipient organization can fix.

For more information, see Error code 5.4.12 in Exchange Online and Office 365.

CCCASV02.CCOUNTY.com gave this error:
SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44919AB3DDCF48A1DC9A721BF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

Diagnostic information for administrators:

Generating server: DM6PR09MB5221.namprd09.prod.outlook.com

Ricardo.Hardy@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44919AB3DDCF48A1DC9A721BF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

Wanda.Walker@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44919AB3DDCF48A1DC9A721BF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

William.Mak@cookcountyil.gov
CCCASV02.CCOUNTY.com
Remote Server returned '554 5.4.12 SMTP; Hop count exceeded - possible mail loop detected on message id <CH2PR09MB44919AB3DDCF48A1DC9A721BF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>'

Original message headers:

```
Received: from BN6PR09CA0004.namprd09.prod.outlook.com (2603:10b6:405::14) by
 DM6PR09MB5221.namprd09.prod.outlook.com (2603:10b6:5:265::23) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.3131.21; Tue, 30 Jun 2020 13:55:33 +0000
Received: from CY1GCC01FT006.eop-gcc01.prod.protection.outlook.com
 (2a01:111:f400:7d02::200) by BN6PR09CA0004.outlook.office365.com
 (2603:10b6:405::14) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend
 Transport; Tue, 30 Jun 2020 13:55:33 +0000
Authentication-Results: spf=softfail (sender IP is 162.217.184.79)
 smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
 header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
```

CY1GCC01FT006.mail.protection.outlook.com (10.97.0.194) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:55:32 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com (10.124.40.39) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun 2020 08:55:08 -0500
Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250) by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:55:08 -0500
Received: from BL2PR09CA0038.namprd09.prod.outlook.com (2a01:111:e400:c743::48) by SN6PR09MB3151.namprd09.prod.outlook.com (2603:10b6:805:e5::32) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20; Tue, 30 Jun 2020 13:55:06 +0000
Received: from CY1GCC01FT005.eop-gcc01.prod.protection.outlook.com (2a01:111:f400:7d02::202) by BL2PR09CA0038.outlook.office365.com (2a01:111:e400:c743::48) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend Transport; Tue, 30 Jun 2020 13:55:06 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79) smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not signed) header.d=none;cookcountyil.gov; dmarc=fail action=none header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by CY1GCC01FT005.mail.protection.outlook.com (10.97.1.1) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:55:05 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun 2020 08:39:57 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250) by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:39:57 -0500
Received: from MWHPR09CA0035.namprd09.prod.outlook.com (2603:10b6:300:6d::21) by MN2PR09MB5451.namprd09.prod.outlook.com (2603:10b6:208:21c::12) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun 2020 13:39:55 +0000
Received: from DM2GCC01FT005.eop-gcc01.prod.protection.outlook.com (2a01:111:f400:7d01::200) by MWHPR09CA0035.outlook.office365.com (2603:10b6:300:6d::21) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend Transport; Tue, 30 Jun 2020 13:39:55 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79) smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not signed) header.d=none;cookcountyil.gov; dmarc=fail action=none header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by DM2GCC01FT005.mail.protection.outlook.com (10.97.3.0) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:39:55 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun 2020 08:24:46 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250) by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:24:46 -0500

Received: from MWHPR09CA0045.namprd09.prod.outlook.com (2603:10b6:300:6d::31)
 by BYAPR09MB3128.namprd09.prod.outlook.com (2603:10b6:a03:a5::10) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.24; Tue, 30 Jun
 2020 13:24:42 +0000
Received: from DM2GCC01FT007.eop-gcc01.prod.protection.outlook.com
 (2a01:111:f400:7d01::205) by MWHPR09CA0045.outlook.office365.com
 (2603:10b6:300:6d::31) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend
 Transport; Tue, 30 Jun 2020 13:24:42 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
 smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
 header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by
 DM2GCC01FT007.mail.protection.outlook.com (10.97.3.159) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:24:41 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
 (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
 2020 08:09:37 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
 by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:09:37 -0500
Received: from CY4PR09CA0093.namprd09.prod.outlook.com (2603:10b6:903:c7::31)
 by MN2PR09MB5515.namprd09.prod.outlook.com (2603:10b6:208:211::20) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20; Tue, 30 Jun
 2020 13:09:35 +0000
Received: from DM2GCC01FT007.eop-gcc01.prod.protection.outlook.com
 (2a01:111:f400:7d01::201) by CY4PR09CA0093.outlook.office365.com
 (2603:10b6:903:c7::31) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.23 via Frontend
 Transport; Tue, 30 Jun 2020 13:09:35 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
 smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
 header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
 DM2GCC01FT007.mail.protection.outlook.com (10.97.3.159) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:09:34 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
 (10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
 2020 08:08:49 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
 by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:49 -0500
Received: from BL2PR09CA0028.namprd09.prod.outlook.com
 (2a01:111:e400:c743::38) by DM6PR09MB3081.namprd09.prod.outlook.com
 (2603:10b6:5:7b::25) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20; Tue, 30 Jun
 2020 13:08:46 +0000
Received: from DM2GCC01FT005.eop-gcc01.prod.protection.outlook.com
 (2a01:111:f400:7d01::200) by BL2PR09CA0028.outlook.office365.com
 (2a01:111:e400:c743::38) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend
 Transport; Tue, 30 Jun 2020 13:08:46 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)

smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not signed) header.d=none;cookcountyil.gov; dmarc=fail action=none header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by DM2GCC01FT005.mail.protection.outlook.com (10.97.3.0) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:46 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun 2020 08:08:11 -0500
Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250) by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:11 -0500
Received: from BN3PR09CA0052.namprd09.prod.outlook.com (2603:10b6:400:3::20) by BYAPR09MB3237.namprd09.prod.outlook.com (2603:10b6:a03:a2::22) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.24; Tue, 30 Jun 2020 13:08:06 +0000
Received: from DM2GCC01FT009.eop-gcc01.prod.protection.outlook.com (2a01:111:f400:7d01::202) by BN3PR09CA0052.outlook.office365.com (2603:10b6:400:3::20) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:05 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79) smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not signed) header.d=none;cookcountyil.gov; dmarc=fail action=none header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by DM2GCC01FT009.mail.protection.outlook.com (10.97.2.68) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:05 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun 2020 08:07:50 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250) by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:07:50 -0500
Received: from CH2PR09MB4491.namprd09.prod.outlook.com (2603:10b6:610:36::19) by CH2PR09MB4395.namprd09.prod.outlook.com (2603:10b6:610:6d::18) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun 2020 13:07:47 +0000
Received: from CH2PR09MB4491.namprd09.prod.outlook.com ([fe80::54b4:1a30:151b:810f]) by CH2PR09MB4491.namprd09.prod.outlook.com ([fe80::54b4:1a30:151b:810f%5]) with mapi id 15.20.3131.027; Tue, 30 Jun 2020 13:07:47 +0000
From: "CCSO Intel (Sheriff)" <CCSO.INTEL@cookcountyil.gov>
Subject: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data
Thread-Topic: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data
Thread-Index: AdZOUZRVrVUDcfOlTiiWh3YE0iFXiAAjZyaaAAALg8I=
Date: Tue, 30 Jun 2020 13:07:45 +0000
Message-ID:
<CH2PR09MB44919AB3DDCF48A1DC9A721BF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>
References: <LYRIS-103909956-1411846-2020.06.29-15.13.38--isp-les-north#lists.illinois.gov@lists.illinois.gov>,<CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>

```
In-Reply-To:
<CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Authentication-Results-Original: cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=none action=none
 header.from=cookcountyil.gov;
x-originating-ip: [162.217.184.194]
x-ms-publictraffictype: Email
X-MS-Office365-Filtering-HT: Tenant
X-MS-Office365-Filtering-Correlation-Id: e59b4440-f289-4c42-0024-08d81cfd418d
x-ms-traffictypediagnostic:
      CH2PR09MB4395:|BYAPR09MB3237:|DM6PR09MB3081:|MN2PR09MB5515:|BYAPR09MB3128:|MN2PR0
9MB5451:|SN6PR09MB3151:|DM6PR09MB5221:
x-ms-oob-tlc-oobclassifiers:
      OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original:
dorE26jV2iSCAAZPeOVhoLD94Hv4kxz7P8odY90Qx9txS684fFRvsQrQNNuMcw5j3CXAvxwJ6RKVNhma4waBTSV
NDGxp/cmBk4EE1mmOJLigUqP/p5XBKfbHvh7l8XKcuXNUZElkV+zSCD0eo8miajinOJW7JVM+LKl83OPl/aGzKO
q6bOCroeq1axlnk4eWaDTHoAOIyh54/JAVk4Vrimq/BMjI4mSCAvqOgQu1CSA3SG/epzZtTashTb6dRWMQgeo+r
JRKNCeaiFc3HMFzVIRVpFATyE6RE6OVqdVOG2K5PsnuO/NhyqisQzWRtPZnKnQE65W6iRiiEbtgObqS5ZzmjcRR
H4CGvuJFl3tG1yM=
X-Forefront-Antispam-Report-Untrusted: CIP:255.255.255.255;CTRY:;LANG:en;SCL:-
1;SRV:;IPV:NLI;SFV:SKI;H:CH2PR09MB4491.namprd09.prod.outlook.com;PTR:;CAT:NONE;SFTY:;SF
S:;DIR:INB;SFP:;
x-ms-exchange-antispam-messagedata:
lfyUdUNo6Rf5kP/RudyGbEyoz+NqqBXdgwdrJdYqEl4KGO77nPkGtTCiHAy0fTDHpKfau4FlsKcP4NPTjBZt0qo
M0swESqf76XMqi53/H/ftP7B223MsFZ9fg5VOxHvc32BClwGPDW+JR3i1qP6YkWVZTuxClUHYV/m3qO/WA7zFrn
q1HGYz/BQ9xQPFzN9ySyJCGd+j9svK3rmnh7njYATQdwBhm/L/06zYHtkcQuXCphogmV5EwxhUeYsDQ18Z9Lphi
UGfntO4ZLeJKhaQlTC86oFyonuAQ8DSt4ZyaYeVXcbNOuyrBFtWcyDVzIMi6RwmDU4aA8eX2yeHjnQ1ngAXfb6w
xmTfCdhMIo3Kbla8ErnlLS56npY6/GW/CGnf1qCGoLMKgNMBwrDrq0yAnvMuo6sEXA/bdkPEDSJD8JxHzl3yOp7
4YkgohRwqBYld6GvNdDvRPJe12IzDacv+MFwLljmdkuIxYJEykmLdGp8GhPL73qvrmFbfbAye08sP
x-ms-exchange-transport-forked: True
x-ms-exchange-transport-crosstenantheadersstamped: CH2PR09MB4395
x-organizationheaderspreserved: CH2PR09MB4395.namprd09.prod.outlook.com
x-crosspremisesheadersfiltered: CCCASV02.CCOUNTY.com
Content-Type: multipart/mixed;
      boundary="_004_CH2PR09MB44919AB3DDCF48A1DC9A721BF56F0CH2PR09MB4491namp_"
MIME-Version: 1.0
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
To: Undisclosed recipients:;
Return-Path: CCSO.INTEL@cookcountyil.gov
X-EOPAttributedMessage: 6
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT009.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(2940100002)(34756004)(356005)(186003)(86362001)(109986005)(166002)(33656002)(82310
400002)(336012)(28085005)(6506007)(26005)(45080400002)(5660300002)(450100002)(9686003)(
83380400001)(21480400003)(81166007)(7696005)(83080400001)(55016002)(19627405001)(525360
14)(1096003)(8676002)(8936002);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 2b67f42c-4bba-4f30-216e-08d81cf695c1
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?o1+pBFwj6bo8wgKCelMNaXOe9qCGT6OpzLS+3IJjEwgEIIK+FAcNHrYl4Ds+?=
 =?us-ascii?Q?YNSCw2Rqy/mzQmlCene7ak0YCR3BkbVVuk6ZZ0jRyFoWv4kMSqIlvzfnkQUQ?=
 =?us-ascii?Q?E1uq2CZP2Th540cgSlCBlQLZiF6R613c7atUuESVNw5XdQYO58zbfjDKB2H4?=
 =?us-ascii?Q?Dl8IrN4ZXIVX/h8jDIfs+SQN8tdFhuoqGcIjWFIcwMSV8Sl6tHuz/zqgFgeW?=
 =?us-ascii?Q?w6jtYH5RY8vF2OiROB9CNK7xz4h/b98E7ORi0T/wA6MAk3R0L/s7YBLUeROD?=
 =?us-ascii?Q?FPx1uJTfOCr3wa34JDDMmPjpSDYYMgBJWQi8JkuVTO4+gGAhSuDZK3Q+5z5r?=
 =?us-ascii?Q?uUs0GjQeJPicGBKB+rgKbyLP0AmdxZXy4YnpK07g1ga0m2r8qtSv6zzBzYCN?=
 =?us-ascii?Q?lp/yoI6IJJl/MREFDctNp0WYi/MUSOJPStx5paF5dFvf6F7E8V9LZvxXR4vn?=
 =?us-ascii?Q?G89zq2GHrKerSi1Y6Rhxtmmv9x78hhG9924NThceYnAQPzZbs0EwVPAV2wvC?=
```

```
 =?us-ascii?Q?z4BG0b5CeTMDUeUWUHCC92l2sMZ2n1wr2oWtGVpL6kFx4eMKJMZJt40dlb3r?=
 =?us-ascii?Q?co4VlQb+jYQm0Ah/5WWT7ZxUUtKyacG1kbaelCvIIx7LluxftN8v4IHWj4kh?=
 =?us-ascii?Q?7pMI1KTkjmv0xfaSMpbuJVOe2B2cfgZg2pPKj0cCS2pgc3UeQu5DTD3ezN7M?=
 =?us-ascii?Q?AZ3wMLgFld7VdRXtHDaLIhOtReQwQ1bx4ZHu6VZNvdoczkzMWSMKXLUmBtbJ?=
 =?us-ascii?Q?XY+VdhzcyrpN3EnpQZw+lF1w3AbeyPNfwaPfv+eUsfUtkWQ6FxUW8yawBnLu?=
 =?us-ascii?Q?tlrS1FoUWWlkF0ax+HVC5fq1uTvPgqGP7+PTi3k2dIyuADRkypQ+t2OiT8PN?=
 =?us-ascii?Q?ywBB3QwFNABupiEEWTJX4P18TwAk125GVYN0AQkTs3yMIq0aHpqaGFydXhkw?=
 =?us-ascii?Q?srnqFmT2A/1SFzuGMdDq+z8LSvbfJw1DihnCP1crfLuRFgIiUEhJcNXUXYf+?=
 =?us-ascii?Q?iq6xP5/n57nf9jqJ8q8EzzsQeSxzZOhhrh1mj1eBQYvjrNBwHezXgjt8/2lM?=
 =?us-ascii?Q?cfFEBukZbN/mtjKJw2rA19L8zOeLUaA+KNjRP9nHHEq1kdIhkhggqGnW0OaW?=
 =?us-ascii?Q?2Zr6w7zd3J8xVOqXAc6TfawVzcWE04K2LB9lN2n1pPfkIf7cgJmK6vxaSGiD?=
 =?us-ascii?Q?RXvVaUJV809oopTW4tWurMNEVvB/J0/pFx/f9A=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: BYAPR09MB3237
X-OrganizationHeadersPreserved: BYAPR09MB3237.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT005.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(19627405001)(7696005)(8676002)(33656002)(8936002)(1096003)(6506007)(52536014)(4508
0400002)(81166007)(83080400001)(356005)(86362001)(83380400001)(5660300002)(166002)(1099
86005)(450100002)(26005)(21480400003)(9686003)(186003)(2940100002)(28085005)(34756004)(
82310400002)(336012)(55016002);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 9a0d0c34-aea1-42ee-e120-08d81cf6a0c5
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?AxXaqsh1rC4lJs7f7ICuLtFSVA5AiGfsM/4Pjjeg4DcMZU8ndOXxb2Nlp3bj?=
 =?us-ascii?Q?No6Xmk88kTXp/imBMUPjJywPliWQcP98McnPQRjCvcH8M8LOZFTmDqbYX/hs?=
 =?us-ascii?Q?8zVKhdd9WMltt3QCum3Sp7wadfiukholdcq2ITWXvKx9YmFX7KuuSXDtDvJS?=
 =?us-ascii?Q?4Eg6e5rhlnEvye/3JVpojlVSezfRO7UwzFTa8vQEoARLJpJXseop61fgr1sg?=
 =?us-ascii?Q?yZe+wgrersaBEKPCWq2xeIQox6o26fEMl+6Zw7Ibip4729/Qx84lCU19Pbmf?=
 =?us-ascii?Q?2ax5FAnw+Xo1mBosKI0Q95ywOO4NK4um7H3uhjZmR9bVDOgoq/h9ggy2bIZu?=
 =?us-ascii?Q?wjlOiVA7BLPfSOvlu49ppBG1OKx/Ne6SB3rlnBJ+YMboFAzyizq0LPzAjYx3?=
 =?us-ascii?Q?ZJTh5iurgm0cc9wDFbPVlsw0/AXP4udaXG8cnKtU87h8cMk8JYHnUwe726cx?=
 =?us-ascii?Q?a+m8tZ3SBuPR4PlPVTsz/vca8qxkvxMA/ZYtoA71qaJabrN0l3vqQEvu/s2Q?=
 =?us-ascii?Q?lyLNHwA8H5d2XcHS0n6BLoky0dc/w1qyuvc4JeQIn8KbY35unnqZtcloeUQ4?=
 =?us-ascii?Q?3phpeibifKAvj5pszNZ5yZ3OkqZtSALqd+I3DRWVdwfYQYMAWFkBDI4RSRY5?=
 =?us-ascii?Q?A5fGS5rCwrh5iyeXvJGl0Y54gR/Dy2A7KXZ1iV58IvfrDhqhX5qdh3/L8Lvw?=
 =?us-ascii?Q?Xxje5QJRKBx3r7W9p1QS3iL7+2B/+m0LnRKKtjIOb0aRzCllOGTLEwxZyfOY?=
 =?us-ascii?Q?o6bZTC9kdqBGok1O6HCnC2weX1gpMdhRcbPgTsGwjHdZru8DA/XP+/v9Tfdd?=
 =?us-ascii?Q?J25iTtnmqmfL4eKbuWtCvt7TiDIH7f5dJ2gJ6xve5lhUWNPtW6UZKkbqaJG0?=
 =?us-ascii?Q?waduATjgRDor3H788eW3SzL3VV0yAjWI0kExk8SUdQLEgTkXqaHPcy1roWmJ?=
 =?us-ascii?Q?8uusZMnpP2P7n0ZdhR1PqKn/+9iK3WkK3X4X95h6yylzaGdKnt82IMzyYkkK?=
 =?us-ascii?Q?qtjHSjS8XBfh1l9HN2M/q8J0oGMUg/a0NVuVCzivwmUwmvM=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: DM6PR09MB3081
X-OrganizationHeadersPreserved: DM6PR09MB3081.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT007.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(45080400002)(450100002)(83380400001)(8676002)(336012)(33656002)(7696005)(830804000
01)(166002)(82310400002)(109986005)(81166007)(9686003)(52536014)(55016002)(26005)(29401
00002)(8936002)(1096003)(186003)(86362001)(5660300002)(21480400003)(19627405001)(650600
7)(34756004)(28085005);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: a1a96dea-0d08-4b55-38e4-08d81cf6b8f0
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?FvmXhdIytius0VSnN8NnqNq16Df1TTscTJCZOZOCHLg8IhK+vuRVhMQGKqIm?=
 =?us-ascii?Q?AGxKjMp5begrhrWxecRBipnDTn9xGGOZT6ccUfZUKwxyrL3CxWcFdDgRCIuk?=
 =?us-ascii?Q?aW9VCeru9yvgD7f2dRTVaAnZhwgJfZA7TJUnkwKPXpKogOEUhGNjnQhukeYp?=
 =?us-ascii?Q?CiN9xdG8TlxLj0LbS7eTqIMWfh8a1b1azzCESCrmHyykRXz0XUaKCcJIzYHP?=
 =?us-ascii?Q?QoxlOLqyvpRQSSczlIBZbZUP04EXUV70F660+rUWBHLfvoB3ALggbL70QTbS?=
```

```
 =?us-ascii?Q?cvX2juxiGmAtNrbvJXaZEW9DW7Nqu7LC4y9CbIDqSzeUd6Vn3+gS9eYDuUZ+?=
 =?us-ascii?Q?R9erPR9O9Hi6ko8aPUeGX8SiyfT6E7rJElDIfrheiFRERFd7j+TV2fImp/ie?=
 =?us-ascii?Q?kXA8qmgwFnXhZrzACY1APpqJZeVUTjCw1UY/Wuv2CNfEoWHEhiTiBdQ3nyox?=
 =?us-ascii?Q?MhRbrJFa4373VPTIWwV4Nis4QZSLPWpXqw5ZYC2ss3VqdtMRPVg8CTp4BfT7?=
 =?us-ascii?Q?JVp9KmTuavqypi41Q5wmrQr9ePF9N3m6pMti3AEzrRBFZEqzOf9TNGYbSq58?=
 =?us-ascii?Q?z9GyhLu/e1WEmWLa3JB0cv0VAnsbu9PsSCKVp/uuQdQVLyFs9ufnGPt5Duw0?=
 =?us-ascii?Q?81g5REfDYbF5HZaNmz03nflRGnvcjkyLQpLkV0SZmQ7X6W9BYY5ApIgCvQN3?=
 =?us-ascii?Q?8HIT/OVkotFbnyiZymZLpjdnGHFNPnkiF8UzbgQoTA0euNjr8XHZarR6XJHc?=
 =?us-ascii?Q?J6x1KPGfw55X8zGvJO98Oxm/Oj/CRo++1/CpPxexTAsVjWWOZ6kwk1QXOb2W?=
 =?us-ascii?Q?cd3xwGIEjJu3JD2SAJnaFhGzmY6MCeA94TXZSxCIwlREDqF+4bhfEWYhQaQZ?=
 =?us-ascii?Q?D/6AcNTkq+zbAetONjAc0mZSRI62ZPFN7eLCCihTh70ohf4+sBPN9dnbSE42?=
 =?us-ascii?Q?Vgs2cSl3tOfX9a8hqe0H9NwHnD0grLPabsi9m8xe4ml03allIr3oeO6L9G5S?=
 =?us-ascii?Q?zy005mee0yURkITE77MOvqQkATLr/zGdXzx5QKzv7McUW+HpFoan083sOmvC?=
 =?us-ascii?Q?fh/JsUbF4YaxEmQy/41sPY9BS1LpDnJraSaZVX9whXy7VhnsTJjV5BMwjXXb?=
 =?us-ascii?Q?blb9MFRzmZkxZbAxlFwxQhbW42VHPJHk4wYSGwmcA2drYmjLYKyLzNWCTTxu?=
 =?us-ascii?Q?V7yWn/rNQIZF8OlkApYQ3+QhQb4eOz+atnElGA=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: MN2PR09MB5515
X-OrganizationHeadersPreserved: MN2PR09MB5515.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT007.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(2940100002)(356005)(34756004)(186003)(86362001)(109986005)(33656002)(166002)(82310
400002)(28085005)(6506007)(26005)(5660300002)(45080400002)(336012)(9686003)(83380400001
)(21480400003)(81166007)(7696005)(83080400001)(55016002)(8936002)(19627405001)(52536014
)(450100002)(1096003)(8676002);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 16cb9bf7-f919-499b-5664-08d81cf6d5d7
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?V1ZRMfnBquy1m2uOtpqWcQf3b7xgJ7H6xJ4A8Iqg1TLVEdBIhuph3n8z5f9K?=
 =?us-ascii?Q?4najk5RqNK+qKuepsmZ052A1gXsGBhXyBkzonvd4DrjLuDlt+atDew0VxIQs?=
 =?us-ascii?Q?8IggQ423t+ipbEVuRw3rIBhwoRDGEHmVv08SK1Oz7mNBPBbILvg3hXi2zf71?=
 =?us-ascii?Q?y+mON7oqldds8pYLpe550sS0MzAJK4fHYnW/AmgCeEWuSawhFyWtmnDSaCFz?=
 =?us-ascii?Q?o04Dp3+/jPPz4k/iTwgj9ZIxMFTjt7/yZ/ZH+UBRfRvo2g9hyKwAhGiePEgw?=
 =?us-ascii?Q?27cNrsfDlywAJvN3A+BHE6yisQm+9p8CnLIVnJcVzygvq6RA9tyEQhvewKtL?=
 =?us-ascii?Q?nIV0TrwG0yjdckHmJceVKWiYdKUYqaw6PGbjjLesMAvKnJ0c88iErS940cZ0?=
 =?us-ascii?Q?USZhFrbMz5u0enVhkQ2y/NnbJkE0DuuvCqO7HOSfZbvR355Tp0I9Cpq2bGLT?=
 =?us-ascii?Q?J0/PtXPxX/HdVInTG4W5eSrnUDC9Fn+8H1zIS0nJPRShnJA7J3q1mLof0zK6?=
 =?us-ascii?Q?HBuyDYRSvE6c46bjjCHM7ezLCPcj9mBAXK7TSk6npxmMmFAN+5BU5khHWRh6?=
 =?us-ascii?Q?f7I2XLe/V/FvXsqHVdYCdTr26OitZPezhVCZzNiw38eifClkQ3OXvGRCCEiY?=
 =?us-ascii?Q?a6hE5dSlIcW8hEmbbiVOistkSg0ZAhhbb31Od/y5CjSe4Pep8pbkSsqoxA4n?=
 =?us-ascii?Q?q33M/vp9oHoFGk4hE9IGIMNqrX0CapkHmvICdhTCs34j9w9FQQLWTE7OBiUt?=
 =?us-ascii?Q?ubj30gTfcMCHkUNH9HM1gI7J5jUdSTytz6lb4cLMrMjG5MBjeG2yLjhLGDmL?=
 =?us-ascii?Q?SGq6XipiRXXU/HPfIuN06k0Tnx8FQXh1Kyi6RCg4oiyRppGv/lQK381OgXR/?=
 =?us-ascii?Q?o/W1YFhs5v/m8esrBcNTRqa50sPRCVr5oeN8+nD6YG04r7oVL+M3OhVfeOSM?=
 =?us-ascii?Q?dnD4R9J75LMH2JhFFShKjrm1PCj+28eDirpr5c3jrEqwjMNgTUKSFpApfAGi?=
 =?us-ascii?Q?838+m2dTJFGIfedGXvK50K8TzQG7OyID/3spIKCd/qmyvLFNdVbdMtXYGNTw?=
 =?us-ascii?Q?g9O5+jjfdLPXqgzGbHJWVezfDN6OhJNSU8GLV8qW+g10EJLfr3/5S70H6Fak?=
 =?us-ascii?Q?75b4Rza4WH7i2vg8pC4zSBS4aW5keW7RJyGQVAO3BJlNi2v4FvMRo9C++wj/?=
 =?us-ascii?Q?tR5t3zU10u0EBOU1FGHgdR2BjEDwcNwNHvmLo59LmXREZ1n21ltmgx9cSL3f?=
 =?us-ascii?Q?NXGcdeNG9PXe3iaUkiQy?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: BYAPR09MB3128
X-OrganizationHeadersPreserved: BYAPR09MB3128.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT005.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(336012)(82310400002)(7696005)(109986005)(356005)(86362001)(6506007)(52536014)(2940
100002)(166002)(450100002)(9686003)(81166007)(83380400001)(83080400001)(1096003)(550160
02)(33656002)(21480400003)(26005)(186003)(8676002)(28085005)(19627405001)(8936002)(5660
300002)(34756004)(45080400002);DIR:INB;SFP:;
```

X-MS-Office365-Filtering-Correlation-Id-Prvs: cdeba52e-b826-46cf-8f93-08d81cf8f284
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?f8pQe3bus+Md2NpdVzA5BUq+jhikwQqS+MBQK/hNSi6uqT/yBL+zy3W+LUSK?=
 =?us-ascii?Q?6RQ7Tjj53u0itrkTahJMu42QQtne3BpkBw6jK3kgLoV2kx/4RVeeM/PQnMsJ?=
 =?us-ascii?Q?zPJVWYEiOYqPca20yNq7heGvYyR8KQ/Z3jwU+S5XpibnriQn4ohhuN0sNJ7h?=
 =?us-ascii?Q?xqEQakeME8GxrEoOzwQb8rABzEWAayY4zuZuZFcgStMMs4p8paf1nO7G88rx?=
 =?us-ascii?Q?Cz0C9YIPjA6x3++muLDiGBM4qNLrm7GeptYXtbncRSw51PjFmeHnqZG3Z89T?=
 =?us-ascii?Q?5qgo8D1kMS5bzveF9Zs3AG1QQzoKXUmFjucRYD/YXDr3HeOFJ0mwv8AgreA+?=
 =?us-ascii?Q?zVtXMSJ1qMI1o1qihJFgjwwOPHNmNvz55Ob7lsY3gGtS3U91MtbqWa0wjgbP?=
 =?us-ascii?Q?qqvLPSyLlHJQsZQyHTaRmPNjHpK3D0E75wmnGxf/hn4hgYcg4dKTFNpOts00?=
 =?us-ascii?Q?Ix86FZX+B7oecfN88faSjc/v4W+LiGkXbPq6ier6GysB5bK8YbpMiX60VnNP?=
 =?us-ascii?Q?NSUB4V66PrWQjXX5VdI7FmiMPS9gOUVaDQZkBOsCH0w2Yp7MC1IboKZ3LEuq?=
 =?us-ascii?Q?DupypW1JvcDkauaWYFgb2GhsxlIePm53Csxbb7/ew82HP6pUYMJjQYSBhpGK?=
 =?us-ascii?Q?I1fU9iKYJDMfydHBIYXxK/Wucmx/Wby6htX4P4wIKUlfNuwRDF1ZI+XFbwHb?=
 =?us-ascii?Q?X92kb2cTaVaYXXMNw3gJRfjp10VM7CTWw/YqsOMFSx/leeu611UHwfdHV21N?=
 =?us-ascii?Q?f9cGsT/FskhTr/ktjrnHwpCfc2D4B7BXQmbc3wDI59KfyxO548wf3avcH5hR?=
 =?us-ascii?Q?1msOnVckpIF+jYzCn8TLjioWGT/Bef43Gt1/l5OHnE5qWo3d+0ToIZf7LeB8?=
 =?us-ascii?Q?bm/XMaQ3AdUNElxsd9fh4r5d42VC5WD8xJWsq9zrJUJjHO0tj84CO92UECUx?=
 =?us-ascii?Q?sQdoG6oMquv5zQP/v9duDqwmxQicbGHUtYYrDinaNwVuyK/l1RZgmq0TBcZx?=
 =?us-ascii?Q?lZx9WLT6AsDGDpfwZHJniW4Qqpf5CPwfYZAW3XqMy/SAwcdt6CT/RZmi+WwG?=
 =?us-ascii?Q?bKfm2e5yZjNcMeR2rvR57Vuo9b/wrRLllnDm+hUtNFZfP5ZBOvT7M9b7xYT8?=
 =?us-ascii?Q?pQI2U2WE5Xqz4WcZA1hYiHAbNHGKuvPgzo1xeXPEyf0YwY6RnIGsgWHotJJC?=
 =?us-ascii?Q?hG5iBpZ/1AzaFuDBVIj2K9KTVKkq9lt06VE6cQ=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: MN2PR09MB5451
X-OrganizationHeadersPreserved: MN2PR09MB5451.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: CY1GCC01FT005.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(8936002)(1096003)(2940100002)(86362001)(186003)(26005)(34756004)(28085005)(1962740
5001)(6506007)(5660300002)(21480400003)(83380400001)(336012)(8676002)(450100002)(450804
00002)(82310400002)(109986005)(52536014)(55016002)(33656002)(9686003)(81166007)(356005)
(7696005)(83080400001)(166002);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: ee2a547d-ab5b-4251-046a-08d81cfb12d3
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?IA8Vknoj1BefsgBsvGGov6i270J8M+CYhTOh/SzNqjb4P4n/rmC8DA6eVLna?=
 =?us-ascii?Q?kGRdfSV8AbNWgHKyxYP+GsEM+IBsYSCO9eoRoPxS6PuAUQvay+cASaC5uTIQ?=
 =?us-ascii?Q?+ATkIyyzebwAXzaobqSguATGk8VJJmKlhUzDId5fOQUFExXqCOO0RC9CxWJv?=
 =?us-ascii?Q?zuAFyDRBK4ZKY8YfpluNACedsV2YcZCR+T1J+XYfMm9X0AoBxK8Qk23Esr1i?=
 =?us-ascii?Q?2OlWYGKutz2bUozIX7RvfBXBh2klO3XXtFychomjjZgGFgiw1hOi4kw7bm+g?=
 =?us-ascii?Q?nPLJdH1cMeeKjo0f0CSQbhhS80SNY0SWQbGrajhddK6/UQdbw6EXB01pAvzW?=
 =?us-ascii?Q?56XfXAiLn0al3Bwe2cftI3GqozZiFtl/Gfie5qC85NrL1B2Eatnh6LbXlggO?=
 =?us-ascii?Q?D+qiaO7xej6xIWjyzrsMBdkcOSgtC4MTUxqh8Bp5bXkGhdCnDiLCz4syEx0E?=
 =?us-ascii?Q?k1r22uDt2Va3awEy85BM4z0zoqvGS9743F4PA9amRUtr6ESmgkNpB4Jg8jjV?=
 =?us-ascii?Q?xk/cgkRTVGXqjfpi5jpBBa8sMOhavaTQI98lOBeaNtdaOFklWc97m9Vr/pWi?=
 =?us-ascii?Q?b46JkxAIWGgjUTX50qqsYDchH4RcCS6b8xpzan0hz+ZdCPPGzlkVj/jGzVN3?=
 =?us-ascii?Q?JC5BYMsUFWoTzdVPXHc3GwDfnPS9MRI++Rti3hKoMPWmiBeAHbHL0LtQilTb?=
 =?us-ascii?Q?5OsoDDesPhFO6Jr2zdU46bgHgaZdbgk9w/BjSI28oGDTVls8q100YSeP9+oB?=
 =?us-ascii?Q?3sIbIyqWyxTBboRakQGAxirrCjqf/AIf4FhBswcBK76R7ev//twQ+iT80LTr?=
 =?us-ascii?Q?W8l+A4uzgeN3LS7l+eVnFYV8epLH4bREL5tenmsIEsZm0qTRXVKNNK1t3mrq?=
 =?us-ascii?Q?zf/6O8MRskjpgghNSUXSiUBR5Wo+iEslblTq8H2vqxBdRO6NvBDI3Mcws8IL?=
 =?us-ascii?Q?9NmkLzx4xhq0Xt/aMESxEaIbgwGwZBVP1lt3wu0DWvB38nmNg9mslq4qHdJg?=
 =?us-ascii?Q?XtDidKGyjHUAaDyj8+6TQ+CFCtz3zhv0D7Ql55I/btcTTMUPmOq6v4A0rb8k?=
 =?us-ascii?Q?JKvFq+707GenPLm3XIx7Ddm8vUj4fucvCxfT70Y3f7bS9NNyWHZd3Mz5+F/x?=
 =?us-ascii?Q?8GSZ0MNzE6M3ziYBjUw9z+VxqvS3xcK9C/N8UsC0zcoLQZEXX3ggXVRzBABF?=
 =?us-ascii?Q?50uif2/h+7NSbeYAI9khOtOtY1ybZM8oWCjTUw=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: SN6PR09MB3151
X-OrganizationHeadersPreserved: SN6PR09MB3151.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com

X-MS-Exchange-Transport-CrossTenantHeadersStripped: CY1GCC01FT006.eop-gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report:
	CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;SFS:(186003)(166002)(336012)(19627405001)(6506007)(450100002)(7696005)(83380400001)(26005)(9686003)(82310400002)(83080400001)(81166007)(86362001)(28085005)(34756004)(52536014)(8936002)(45080400002)(5660300002)(109986005)(2940100002)(21480400003)(55016002)(33656002)(8676002)(1096003);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs:
	01e94b24-f074-4a45-1f3d-08d81cfd31bf
X-Microsoft-Antispam: BCL:0;
X-Microsoft-Antispam-Message-Info:
	=?us-ascii?Q?at7gbnaTSLH8A5cbAl/ZJr4t9MfWOWoGXtAgigIMxAj7L4hR/yKXJrIiB6A4?=
 =?us-ascii?Q?g0Mv5c1GYix4qt3LdEm2nAVAgs6b1T2YXHmJIFpjtvO7pKSJZV+8fJuFfIDr?=
 =?us-ascii?Q?KwMi+aYTT1TVZgKNS1+cmFhIYAXUlljq+3wBZu+16CfWXzaYX2RHF9humurj?=
 =?us-ascii?Q?N8ipQhcnOs4ES/jMzCvELptR1d6ECQHKNJqCNjuWQSegrt7mMH9PWbrOaAoC?=
 =?us-ascii?Q?5sds6MmjVI3k/FnEqWwW4gq5R8KYGGvWITREWuW5myG6jcT7VklL56d7Ep4w?=
 =?us-ascii?Q?wSqLzAJ6HXRrA9CtstrfMHuABuwDFLINFY/TcQc5AMPydmbumrCPsEa6Yq3O?=
 =?us-ascii?Q?AOakeSZMFvLzEFWfjUxdJnxbo4YGO7TGeqNDJLgzlECZcJURWJNU8+hlkdPQ?=
 =?us-ascii?Q?zX+GItRjm1hDfQeZJJfMa3QGJPL/ace2afGbFMgc9+4iIxn7fHUIS59StZ9G?=
 =?us-ascii?Q?vST/rrBu9cZ4LDekBF12XPl5OzBvOZ2i0aZn85HGse92mhMAl2YcngxZe/W6?=
 =?us-ascii?Q?l1oVvkjqJPS7djpC/zF5g8fjSAyVt+1MpcyLoaUrn+Qpt+7AWS33sMB7KRut?=
 =?us-ascii?Q?VXrFJFxGlBLSdpLo87dafpExFu76in2+SyQuHUho/w4NHbembJqWy/fKwwiG?=
 =?us-ascii?Q?iJnN+Pwf3ke4fOPabeuHvlnDHDcP5iZAVHfFCNE3EM03foqcnNtYFWQpY8xH?=
 =?us-ascii?Q?p0xAIvtR40J1ZfHGEx7FD0NOicxM5NJCGCqCOibRFzT/zXynYTydROuMa05G?=
 =?us-ascii?Q?UjdSFZEB2+FWpH1cx3EnyqeWfC8YfAU61YL8dfIMiWzKyfdQ8cA1D9a8ArlP?=
 =?us-ascii?Q?p7Rgr6O8tzN/5jcauhxzA2bvDmDp43G07ZxIIzYZMTAJfX9erPwQe/5XSPXg?=
 =?us-ascii?Q?5SHpbJq2YLjrGOoprU/WF0afreMVfbTscKIeCmwvyaoPzPd0vyZDSMhorI7P?=
 =?us-ascii?Q?L0zBJfDhAMp4P4kQnIpAA6HAUssMzrDjKI0z7PFWSsidmotK7QM5KZ5X0S/H?=
 =?us-ascii?Q?fklLRuZz5av3twkxxRAhFQzK1XBsnWvBZkpS/jWoPU+KL5bUniW/1t3vNM5E?=
 =?us-ascii?Q?OpFsqDhILsJ/2hsTM7DX4WQXVWfXAX1VMsr3e91nyfMyuZ5uLfKAqujWeHQ1?=
 =?us-ascii?Q?pASWdVh4EEs10XdZnbh2PZqF6yz6quRcDlQc+cH5PPneE9OUYkAQOdt1fV/0?=
 =?us-ascii?Q?eUxpX7ltwPwDHicq3ivc2oo7FiYVSuqNLiscUA=3D=3D?=
X-OriginatorOrg: cookcountyil.gov
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 30 Jun 2020 13:55:32.4088 (UTC)
X-MS-Exchange-CrossTenant-Network-Message-Id: e59b4440-f289-4c42-0024-08d81cfd418d
X-MS-Exchange-CrossTenant-Id: 8b4d55ae-6db4-4e05-a85c-59d6a256cd6e
X-MS-Exchange-CrossTenant-OriginalAttributedTenantConnectingIp: TenantId=8b4d55ae-6db4-4e05-a85c-59d6a256cd6e;Ip=[162.217.184.79];Helo=[CCCASV01.CCOUNTY.com]
X-MS-Exchange-CrossTenant-AuthSource:
	CY1GCC01FT006.eop-gcc01.prod.protection.outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Anonymous
X-MS-Exchange-CrossTenant-FromEntityHeader: HybridOnPrem
X-MS-Exchange-Transport-CrossTenantHeadersStamped: DM6PR09MB5221
X-OrganizationHeadersPreserved: DM6PR09MB5221.namprd09.prod.outlook.com
X-CrossPremisesHeadersFilteredByDsnGenerator:
	DM6PR09MB5221.namprd09.prod.outlook.com

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	CCSO Intel (Sheriff) <CCSO.INTEL@cookcountyil.gov>
Sent:	June 30, 2020 8:07:45 AM CDT
Received:	June 30, 2020 8:55:33 AM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

Please see the attached DHS Intelligence Brief, “Criminal Hackers Target US Law Enforcement Data,” dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

If you no longer wish to be on this distribution list, please send an email to ccso.intel@cookcountyil.gov to discontinue receiving these emails. If you would like any member under your command to receive these emails, please send an email to ccso.intel@cookcountyil.gov and include their name, title and email address in the body of the request.

Cook County Sheriff's Office
Strategic Operations Center
3026 S. California Avenue
Building 5, 2nd Floor
Chicago, IL. 60608
Office: 773-674-2694 or 8477
Fax: 773-674-4797

THIS IS A CONFIDENTIAL LAW ENFORCEMENT COMMUNICATION. The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential. If you are not the intended recipient of this message, or if this message has been addressed to you in error, please immediately alert the sender by reply e-mail and then delete this message and its attachments. Do not deliver, distribute, transmit or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action relative to the information contained in this communication and/or attachments. This e-mail and any attached documents may contain For Official Use Only and/or Law Enforcement Sensitive material and should not be disseminated outside of official law enforcement channels. The information contained in this message as well as any attachments shall not be released to the media or the general public.

Undeliverable: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	Microsoft Outlook <MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@cookcountyil.gov>
To:	CCSO.INTEL@cookcountyil.gov, Alexander.Brodie@cookcountyil.gov, Lisa.Farinella@cookcountyil.gov, Kevin.Graff@cookcountyil.gov, Kevin.Cooper@cookcountyil.gov, Kevin.Christofidis@cookcountyil.gov, Kelly.Sweeney@cookcountyil.gov, Jonathan.Mobley@cookcountyil.gov, John.Steed@cookcountyil.gov, John.Pradun@cookcountyil.gov, Jeffrey.Pasqua@cookcountyil.gov, James.Scannell@cookcountyil.gov, James.Hughes@cookcountyil.gov, Lissette.Rivera@cookcountyil.gov, Giovanni.Veitkus@cookcountyil.gov, Gary.Newsom@cookcountyil.gov, Frank.Caridei@cookcountyil.gov, Felix.Arvelo@cookcountyil.gov, Diane.Haras@cookcountyil.gov, David.Delgado1@cookcountyil.gov, Daniel.Strong@cookcountyil.gov, Daniel.Burke@cookcountyil.gov, Cedric.Mccloud@cookcountyil.gov, Catherine.Domine@cookcountyil.gov, Anthony.Burns@cookcountyil.gov, Gary.Rizzo@cookcountyil.gov, Luis.Santoyo@cookcountyil.gov
Sent:	June 30, 2020 8:55:43 AM CDT
Received:	June 30, 2020 8:55:46 AM CDT
Attachments:	Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

Delivery has failed to these recipients or groups:

Alexander.Brodie@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Lisa.Farinella@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Kevin.Graff@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Kevin.Cooper@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Kevin.Christofidis@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Kelly.Sweeney@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Jonathan.Mobley@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing

configuration or mailbox rule setting. If the problem continues, contact your email admin.

John.Steed@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

John.Pradun@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Jeffrey.Pasqua@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

James.Scannell@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

James.Hughes@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Lissette.Rivera@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Giovanni.Veitkus@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Gary.Newsom@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Frank.Caridei@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Felix.Arvelo@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Diane.Haras@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

David.Delgado1@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Daniel.Strong@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Daniel.Burke@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Cedric.Mccloud@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Catherine.Domine@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Anthony.Burns@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Gary.Rizzo@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Luis.Santoyo@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

The following organization rejected your message: CY1GCC01FT007.mail.protection.outlook.com.

Diagnostic information for administrators:

Generating server: CCCASV02.CCOUNTY.com

Alexander.Brodie@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Lisa.Farinella@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Kevin.Graff@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Kevin.Cooper@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Kevin.Christofidis@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Kelly.Sweeney@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Jonathan.Mobley@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

John.Steed@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

John.Pradun@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Jeffrey.Pasqua@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

James.Scannell@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

James.Hughes@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Lissette.Rivera@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Giovanni.Veitkus@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Gary.Newsom@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Frank.Caridei@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Felix.Arvelo@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Diane.Haras@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

David.Delgado1@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Daniel.Strong@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Daniel.Burke@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Cedric.Mccloud@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Catherine.Domine@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Anthony.Burns@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Gary.Rizzo@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Luis.Santoyo@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Original message headers:

```
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
 (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
 2020 08:40:41 -0500
```

Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
 by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:40:41 -0500
Received: from DM6PR09CA0009.namprd09.prod.outlook.com (2603:10b6:5:160::22)
 by DM6PR09MB4936.namprd09.prod.outlook.com (2603:10b6:5:267::11) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
 2020 13:40:38 +0000
Received: from CY1GCC01FT010.eop-gcc01.prod.protection.outlook.com
 (2a01:111:f400:7d02::209) by DM6PR09CA0009.outlook.office365.com
 (2603:10b6:5:160::22) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
 Transport; Tue, 30 Jun 2020 13:40:38 +0000
Authentication-Results: spf=softfail (sender IP is 162.217.184.79)
 smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
 header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
 CY1GCC01FT010.mail.protection.outlook.com (10.97.0.149) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:40:38 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
 (10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
 2020 08:40:06 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
 by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:40:06 -0500
Received: from MWHPR09CA0026.namprd09.prod.outlook.com (2603:10b6:300:6d::12)
 by DM6PR09MB4838.namprd09.prod.outlook.com (2603:10b6:5:265::20) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20; Tue, 30 Jun
 2020 13:40:04 +0000
Received: from DM2GCC01FT005.eop-gcc01.prod.protection.outlook.com
 (2a01:111:f400:7d01::209) by MWHPR09CA0026.outlook.office365.com
 (2603:10b6:300:6d::12) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
 Transport; Tue, 30 Jun 2020 13:40:03 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
 smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
 header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by
 DM2GCC01FT005.mail.protection.outlook.com (10.97.3.0) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:40:03 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
 (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
 2020 08:24:59 -0500
Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250)
 by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:24:59 -0500
Received: from BN6PR09CA0066.namprd09.prod.outlook.com (2603:10b6:404:7a::28)
 by DM6PR09MB4591.namprd09.prod.outlook.com (2603:10b6:5:1b9::10) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
 2020 13:24:57 +0000
Received: from DM2GCC01FT008.eop-gcc01.prod.protection.outlook.com
 (2a01:111:f400:7d01::209) by BN6PR09CA0066.outlook.office365.com

(2603:10b6:404:7a::28) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
Transport; Tue, 30 Jun 2020 13:24:57 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT008.mail.protection.outlook.com (10.97.3.193) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:24:56 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
(10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:09:46 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:09:46 -0500
Received: from CY4PR09CA0087.namprd09.prod.outlook.com (2603:10b6:903:c7::25)
by BY5PR09MB5777.namprd09.prod.outlook.com (2603:10b6:a03:246::8) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
2020 13:09:41 +0000
Received: from DM2GCC01FT007.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::208) by CY4PR09CA0087.outlook.office365.com
(2603:10b6:903:c7::25) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend
Transport; Tue, 30 Jun 2020 13:09:41 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT007.mail.protection.outlook.com (10.97.3.159) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:09:40 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:08:34 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:34 -0500
Received: from BL2PR09CA0033.namprd09.prod.outlook.com
(2a01:111:e400:c743::43) by MN2PR09MB5785.namprd09.prod.outlook.com
(2603:10b6:208:21f::20) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20; Tue, 30 Jun
2020 13:08:30 +0000
Received: from DM2GCC01FT005.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::205) by BL2PR09CA0033.outlook.office365.com
(2a01:111:e400:c743::43) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend
Transport; Tue, 30 Jun 2020 13:08:30 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT005.mail.protection.outlook.com (10.97.3.0) with Microsoft SMTP

Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:30 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:08:21 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:21 -0500
Received: from BL0PR0901CA0030.namprd09.prod.outlook.com
(2603:10b6:208:1c0::40) by SA9PR09MB5230.namprd09.prod.outlook.com
(2603:10b6:806:45::10) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.23; Tue, 30 Jun
2020 13:08:19 +0000
Received: from DM2GCC01FT006.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::203) by BL0PR0901CA0030.outlook.office365.com
(2603:10b6:208:1c0::40) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
Transport; Tue, 30 Jun 2020 13:08:19 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT006.mail.protection.outlook.com (10.97.3.107) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:19 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:08:15 -0500
Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:15 -0500
Received: from BN3PR09CA0064.namprd09.prod.outlook.com (2603:10b6:400:3::32)
by SA9PR09MB5168.namprd09.prod.outlook.com (2603:10b6:806:41::12) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20; Tue, 30 Jun
2020 13:08:11 +0000
Received: from DM2GCC01FT009.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::207) by BN3PR09CA0064.outlook.office365.com
(2603:10b6:400:3::32) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20 via Frontend
Transport; Tue, 30 Jun 2020 13:08:10 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT009.mail.protection.outlook.com (10.97.2.68) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:10 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
(10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:07:54 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:07:54 -0500
Received: from BL0PR0901CA0023.namprd09.prod.outlook.com

(2603:10b6:208:1c0::33) by DM6PR09MB3225.namprd09.prod.outlook.com
(2603:10b6:5:35::33) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
2020 13:07:51 +0000
Received: from DM2GCC01FT006.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::205) by BL0PR0901CA0023.outlook.office365.com
(2603:10b6:208:1c0::33) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend
Transport; Tue, 30 Jun 2020 13:07:51 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT006.mail.protection.outlook.com (10.97.3.107) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:07:51 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:07:26 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:07:26 -0500
Received: from CH2PR09MB4491.namprd09.prod.outlook.com (2603:10b6:610:36::19)
by CH2PR09MB4395.namprd09.prod.outlook.com (2603:10b6:610:6d::18) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
2020 13:07:22 +0000
Received: from CH2PR09MB4491.namprd09.prod.outlook.com
([fe80::54b4:1a30:151b:810f]) by CH2PR09MB4491.namprd09.prod.outlook.com
([fe80::54b4:1a30:151b:810f%5]) with mapi id 15.20.3131.027; Tue, 30 Jun 2020
13:07:22 +0000
From: "CCSO Intel (Sheriff)" <CCSO.INTEL@cookcountyil.gov>
Subject: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement
Data
Thread-Topic: Pass Through - (U//FOUO) Criminal Hackers Target US Law
Enforcement Data
Thread-Index: AdZOUZRVrVUDcfOlTiiWh3YE0iFXiAAjZyaaAAAHqe8=
Date: Tue, 30 Jun 2020 13:07:20 +0000
Message-ID:
<CH2PR09MB4491104495F32B729B402EA7F56F0@CH2PR09MB4491.namprd09.prod.outlook.com>
References: <LYRIS-103909956-1411846-2020.06.29-15.13.38--isp-les-
north#lists.illinois.gov@lists.illinois.gov>,<CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH
2PR09MB4491.namprd09.prod.outlook.com>
In-Reply-To:
<CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Authentication-Results-Original: cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=none action=none
header.from=cookcountyil.gov;
x-originating-ip: [162.217.184.194]
x-ms-publictraffictype: Email
X-MS-Office365-Filtering-HT: Tenant
X-MS-Office365-Filtering-Correlation-Id: d60cf752-ee33-4157-39fc-08d81cfb2cb5
x-ms-traffictypediagnostic:
CH2PR09MB4395:|DM6PR09MB3225:|SA9PR09MB5168:|SA9PR09MB5230:|MN2PR09MB5785:|BY5PR09MB577
7:|DM6PR09MB4591:|DM6PR09MB4838:|DM6PR09MB4936:
x-ms-oob-tlc-oobclassifiers:
OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;
X-Microsoft-Antispam-Untrusted: BCL:0;

X-Microsoft-Antispam-Message-Info-Original:
i+uzE6hVIcnRsGS1QWcn6TsXKHhKrGB2ApYs8WShxLg2UpOu82OHRfhsFp+9CjlQecvSzZCwXpa1AWO4qrntWsl
2q6Qw2oMnjCqqm1vLhbB607gMDIp2f7mBL3QYwDQr+r4wNnGRAC9xe3+5GPOy8gs0xnYC/tzY345eFTIOdpxi8h
rvmE/ovgAyrKD2M+aVOHraAlD6Yg0/dp+AIa6uQJHM92dDHc+v9NmfffieN4nF9HU5Sho5QfaoyzaceI9B/Iqgk
rVdjSZovu2pQFCekwDl0jsQ53n+eomH8b9QGuQEKneL2evjWMOddw0zd2moDdY/WDuTaKA+WaJWmCPW1pOPTjZL
1592rts6hC49p2A=
X-Forefront-Antispam-Report-Untrusted: CIP:255.255.255.255;CTRY:;LANG:en;SCL:-
1;SRV:;IPV:NLI;SFV:SKI;H:CH2PR09MB4491.namprd09.prod.outlook.com;PTR:;CAT:NONE;SFTY:;SF
S:;DIR:INB;SFP:;
x-ms-exchange-antispam-messagedata:
BuYbw0RoSBfECmAFs5sfpqFR/eESsNr+Plx06kdsYiyNoXFEYgS3Jz6QYqBwqda1BgTm5iebI1sncXRB6v4+RaV
C42PElOHwFJBOAzNHKMxkCZCwRx1mubguafevanh98UlGYiSoqtiVFIMyzzqWjVwq2ALgG6TEoWTOD6wL3DH1g+
twaRUDU5pX7Y3UuqHnjSUkkWpE3g+KMrlKiWDb6hsqAZsExSu0dRsfe1bY5iawMgV1P06KM54AE4iNVyJ6s+PhZ
oFB021MJN0zbzrKRmG5l76nAVkDQZ6LAJ59qRaYnm4V2jeg+UrmezaEA1BSTXRnJE7c4PTWoAZR7vsnGJlZPDSr
wlqBu5V9fQ0asbFFrSOauG9RYEIceEBMj2qfNX9W5sCwVf+Z2W+dW0tMy5YgF7ghw6XrerqzMMShABB14TwG3sg
hMkbytZTnSmqwnqf05E2cPgyZHNVzIQHTfXbIbLbhC/u0Vat8cAb+p0h0NzcOhHtduUMJV/CgNncT
x-ms-exchange-transport-forked: True
Content-Type: multipart/mixed;
	boundary="_004_CH2PR09MB4491104495F32B729B402EA7F56F0CH2PR09MB4491namp_"
MIME-Version: 1.0
X-MS-Exchange-Transport-CrossTenantHeadersStamped: CH2PR09MB4395
X-OrganizationHeadersPreserved: CH2PR09MB4395.namprd09.prod.outlook.com
To: Undisclosed recipients:;
Return-Path: CCSO.INTEL@cookcountyil.gov
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-EOPAttributedMessage: 7
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT006.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(34756004)(28085005)(45080400002)(9686003)(8676002)(166002)(8936002)(1096003)(55016
002)(81166007)(7416002)(83080400001)(52536014)(26005)(7696005)(19627405001)(86362001)(2
1480400003)(356005)(82310400002)(2940100002)(33656002)(336012)(450100002)(109986005)(56
60300002)(186003)(83380400001)(6506007);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 03205142-5935-4a88-f6ba-08d81cf68713
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?qqz2axaPsPt6cRhwprV+ioE4yFXF9neuz1x680KXimBZbJL5qP5Myc39zAlO?=
 =?us-ascii?Q?zON93FB/g/7egToohlpauUHr4xPFTLzJc8KfE9nIvBojS2dKYkZG0AAhJ/V0?=
 =?us-ascii?Q?l9s6wqLFJ4LQMzyaU4uFCavEdnOoembTpISLdDi/DsZ3XWoCOP/CsmwBbapP?=
 =?us-ascii?Q?i3zuVExuALmj1CD1txkMREfYV3NoGgazwkweui2VjMTubkYGoHpiPsnfpFKj?=
 =?us-ascii?Q?BcWkcx7tg79Kw1xWUmKAeAD1DQ6oEAGEb0S7nMA2Yt+/hJURVhFFm0esqbNN?=
 =?us-ascii?Q?mkHh8B6oSqixPVXWx7wk2CAFrZIIIVMqQLHdTLu3HK0lIeosglyNQaniTmwA?=
 =?us-ascii?Q?WXs6y7ZCIEqNFeFlMT721cipk9/QpeIPxQgTsNpxzPJUyYADYoSwlmC+UQHW?=
 =?us-ascii?Q?rXjWLAebvMpJGwyWgjAlXceB+qx8bksgdSGO0CD5a1bP2I1lelQeE/Aa8ThE?=
 =?us-ascii?Q?NvTxMZLlJUnmoV+gwu/uKUbuEUz6aEP8nxqEjU5hxRX+RtdZqOSbtDr7WpHk?=
 =?us-ascii?Q?BvBpE59n5Z6upE6BOkOo8ryPyTLCkeNNT3Jr05+ME7qeraotItp1VtlXc5fD?=
 =?us-ascii?Q?aV11KxWYdde1poCRiIHRSGLGBQwzMORuHrmKSWgjb2QHXAyVuIeMzlT91Jav?=
 =?us-ascii?Q?DQCycNLmNDRjb0FArmuR+RSCLQcSa7Y3f1qMWS4Prb04kgJrD+8/ccgHayF0?=
 =?us-ascii?Q?v4PlKvLymI9l99+BhrBJhvtfRpOvDUbm/BVRnuY7sykmEjtAkSJPgtX12wQ4?=
 =?us-ascii?Q?77mznmNzDLm/i/aA4ZP+alx1nKfejDumwctuLmv3FvGFyftlCWWQbQ2R6tR3?=
 =?us-ascii?Q?gkkTouT6a40t3tDdfzdMIUfMauxg50MfFkFtYpygOT/YMtYXDvjQOh0P5Aib?=
 =?us-ascii?Q?1O0MtEsOGpGhyn7lDXIQhztnMPSKb1Ky4ZuBXKloLqMyQJg/LgwJ9IvNGcRg?=
 =?us-ascii?Q?+ua3FbBZLPTbQI/gRkoofEwyeTBQhOttXwmU5gIwWhS61/AQdD+nkCMp53XS?=
 =?us-ascii?Q?pfwfrOMmqGLZ74i+Ma0jvaYQkcp6sknCUKZibUOaA6gS4cdhLHcAhZ0NdtU2?=
 =?us-ascii?Q?/fuUVt/hcqdcf1i1qU3cNda7KyMrw6OGLPPLAlyeZ+gq1mi8OX2eiSnmGkEd?=
 =?us-ascii?Q?JgUSd+3E+iq7zXi8E+oic7eQ6I7H8/OrvrGoUbxToDFP0in/nSyl730Gk2Et?=
 =?us-ascii?Q?M00lE8+QcBNaPYdP38w1YV/mMjVrdFNMacH8vA=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: DM6PR09MB3225
X-OrganizationHeadersPreserved: DM6PR09MB3225.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT009.eop-
gcc01.prod.protection.outlook.com

X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;SFS:(109986005)(86362001)(83380400001)(166002)(5660300002)(21480400003)(82310400002)(81166007)(2940100002)(83080400001)(28085005)(34756004)(26005)(450100002)(9686003)(186003)(336012)(55016002)(7696005)(19627405001)(52536014)(6506007)(8676002)(8936002)(1096003)(7416002)(45080400002)(33656002);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 0e133ae1-4d70-4c57-3dfa-08d81cf69835
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-ascii?Q?eVb9CDSfm7BNFNbT91jGqNfAedtAy+gYwb1BEQ8yhaqNd3a1RQpq6gwtLiTL?=
 =?us-ascii?Q?7Bilm9qpTeSie4GROzb6dV2eUvTKysrTe4ESZB5AEFQYs9ddXwbqz9G6/ThH?=
 =?us-ascii?Q?H89PT+AU6krnlDvEOpW4/JBJNjdVCwrouuTbeJTXBynVbza640ZA1YkawWK/?=
 =?us-ascii?Q?HrAnBYnGWAWF9jtDi7t3MHrkcM1ytpFTLIl4C17YoZk09iGBO3Ptp4s1Ljse?=
 =?us-ascii?Q?BFbPbObAYwTgjk1Qr+WtC4Qhs1Su82SEhMSb9mCKnrSWyDkj47RcyV4z8Zen?=
 =?us-ascii?Q?lGcVm53vT6jMLmOC75uV/l2KA6VKEhO7xeLixpJwnaXgj1Av7sr1p66x1yi7?=
 =?us-ascii?Q?yRxeCaG0RFT+6lsuYs5mlYUitXbrZuRYzbUneoHQeQbHFZmZGgZDlLuHrN9B?=
 =?us-ascii?Q?sso+dBmmmVBG8lFlrOFzer9DB6BpQtP7+qUGSsWfPmNjS7H7HfcRSJrxgmHn?=
 =?us-ascii?Q?eUxlpTp3hDsgCQrqwuXdu8slIFuxwJ72px7r5HOawG0QgGfi6tJfuugTyxBX?=
 =?us-ascii?Q?tKamJyXzJfrDQoRk63GHGPgTVGVih7u/+ybUQeLBGUdIGzoEtlZZUgcWRQdi?=
 =?us-ascii?Q?66W9ktm4FOBws3cYNIFh67n0Oeo1K5m9LOJKiTIIoWcfUOBv6K/J4Bywd4TQ?=
 =?us-ascii?Q?23A3lb9uWY9X3dIa+/wFt0kqqArAHNLYY8YlRxw4bX/UNtKqb18nfnVx9M7K?=
 =?us-ascii?Q?nxS2QmmO4aK2NMKJSBO8s3kUFK3+EQCZnfbAYIAVR4jzDL42cJPz7qLTCeAC?=
 =?us-ascii?Q?uh6KI/izKS4LvcUezEJt3mab0t3EIHVp2SFYQVndbPRWaGtAuP+yp7knXsGX?=
 =?us-ascii?Q?AATNK8YBw4t6A6tt1RtDY3wXEOnaIZiOWZoPZqSa/zYNkZHmcXW/Win5gdbS?=
 =?us-ascii?Q?c1ooH8zRhhLLvX0buENIjGmMM5A7Gl/096VMGI6GlD1xPQ/xTOCy0JlXnzPe?=
 =?us-ascii?Q?L7fJ9rSJ7xHMDkbUv5uefdc42q+SwN/SRJ7EpV5Bh5ZHncjl+SfEldkYznbu?=
 =?us-ascii?Q?vHmiPLP+MQN6Rx+/TX+a8FeIHzhFOUspYAXtt3mBAk8dzd35Q0jqVLTOygxF?=
 =?us-ascii?Q?6T1+9b9Ofm0lLZLG7Wlyd8bx7jBC3L0uWphR2rYb5TX1qf5nn1a6ehVr1RBH?=
 =?us-ascii?Q?G9p182t9vn3a8WzKr0W7/1bu2YpxOU19I7Bim1VjedBOmiyxcidURyWoS1O0?=
 =?us-ascii?Q?DnOPxDMxxFN4YnZcSTc4RyT414tcBFAHXl5RT1rxAH3dVbhydRhOk7p43zPZ?=
 =?us-ascii?Q?yWJncx4mwKr7FSdc/ZnD?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: SA9PR09MB5168
X-OrganizationHeadersPreserved: SA9PR09MB5168.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT006.eop-gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;SFS:(186003)(166002)(83380400001)(356005)(86362001)(82310400002)(19627405001)(830804000 01)(81166007)(5660300002)(55016002)(109986005)(450100002)(33656002)(9686003)(52536014)(2940100002)(7416002)(21480400003)(8676002)(26005)(28085005)(34756004)(6506007)(7696005)(336012)(8936002)(1096003)(45080400002);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 3cd88b13-bc33-4696-34e3-08d81cf6a3c1
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-ascii?Q?gFqiaJZmTC0mLWk4LRgXhDnPPyiiiqa/WHf/4axTrYiPmVu53WjjWqfXA2s1?=
 =?us-ascii?Q?omlwpkVgtY4OTgU49EWCuNOeN+hRoyD/vqcjWc6UupeNqhTe4rmW8+r2Q+Z1?=
 =?us-ascii?Q?N2znXaAvLRPQQyx5ea7uWVM1h9zZvlEIM3/5oDyQF82iQE2Ijiff46861UCr?=
 =?us-ascii?Q?ntGGTp8+JyerJkwrDfZzW9Rn6RsqOq1t/Njt5GwKLSNfIdHXO0ZVOw417hMZ?=
 =?us-ascii?Q?vQvku4wehAy7N3QjDJkfoQ3eN6rmFyCwYn2YHVUDvXV6VSwr69GeCutDuNPc?=
 =?us-ascii?Q?9Lbea71GbUlyG/YWK7hEnceWhHJPB95Y/MZuNTr9qhsqhXBE/H8AYIewIY8I?=
 =?us-ascii?Q?ujtStONT8tlQ2TOaX+gQYFl5HX/yOiU5JAaYZ6+GW7l+n9PSmjqTkaIAhO54?=
 =?us-ascii?Q?hPEkWFnrHB4HjtH9GUPtOS+FryJHF0XEHiiSb6vPQ2bwAW8DjE+xVHhzHlHj?=
 =?us-ascii?Q?TLPKI47cDL6wKxuYZWSa+DvPZ5FSbc3qbLJVNWnFKz0jDOPO8VkL2WG98Fql?=
 =?us-ascii?Q?YlqaRF51FJa3zjKMsvXGKyUu/yfRW+Nt9xeBDeQYjjsUpnRuH+fJHKXvhxM9?=
 =?us-ascii?Q?LsWI6nu4zaYA35f6tjM4tOK7Wi9z0reVcNHzKYCH5oi45LQHV+8Fi3+MA3N3?=
 =?us-ascii?Q?ZUtVLKWx/dmihfKWUs+4q8hkXd2UR8JE/2CPdqRjL7z/mndXWuWSwdPuPPSj?=
 =?us-ascii?Q?D+NxZvfgfr0Uf55UQ7WJhflYdsGHUyJiSGjUUPTexcH8UHZ1XxS9qDGXrWRq?=
 =?us-ascii?Q?+kTOrkhtZahg0mIPvY9ai1e03gAKUwcM6/0MnWIrkiowo0hFB6sAv/XuKDZx?=
 =?us-ascii?Q?/MLCbEtzZscIXRSy0VeAvS2dMwMPPAbxB3ivoOts8ghvfeX6iNib/DBc96uZ?=
 =?us-ascii?Q?LawIoMuFoi9PQIAh3rLJ1kPiujtcJlCuz/vEkYQKOEXJOgJUQ2kFJLM0aTCG?=
 =?us-ascii?Q?xZ9V6f8QLFnVi6nq9SnzNghh4CLuR3FsmWd/K+SPQu+udweYxtreGeFaFavO?=
 =?us-ascii?Q?IB/Z6zBXrcJn/BdR+WHKGuMSW6gqt1QsIYv511y8d2+vERI4aFUtSeFmeLiF?=
 =?us-ascii?Q?CiPmLPr04SWwKs/DoN3sdlXtDqsWN9WlLHZXBAEx3vOLK3HEfTRIkI9sIhMX?=
 =?us-ascii?Q?wFEvEZINweoU4GO9lFa9YTFlS9uHZavmiYXoKJ2jhRXKTVIc0vsTyEKWPYsW?=

```
 =?us-ascii?Q?OhL+iOCLD30MFSfVemx3t6sGOAoGcYZSIgXgZA=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: SA9PR09MB5230
X-OrganizationHeadersPreserved: SA9PR09MB5230.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT005.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(26005)(6506007)(336012)(55016002)(450100002)(8936002)(1096003)(45080400002)(214804
00003)(86362001)(7416002)(7696005)(5660300002)(52536014)(28085005)(34756004)(2940100002
)(166002)(33656002)(83380400001)(82310400002)(186003)(9686003)(8676002)(83080400001)(81
166007)(19627405001)(356005)(109986005);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: d74b9e8a-9638-4e50-af52-08d81cf6a8b4
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?ATn/9yDjsTyufQcLvFwtmp4bayBZ0x1EY4Vu3mFfGw51mZnmn8Ud74rrOOcD?=
 =?us-ascii?Q?nwU7lM79KWKXrMFiI0JfADwWfcsXhG90cUjijIojD/uL35mDUZf7L7POrThF?=
 =?us-ascii?Q?VAtwzzea1FoibDsdjsY26Xkn7CCijep071WomNz1P3HGntcwR6NLRrbJuWbt?=
 =?us-ascii?Q?gHO0ZouvsN/rg70kX3t6/9CY2bsJUdcClfWzfkBlqCnUe5dc7vSwMAYj2f4r?=
 =?us-ascii?Q?gKzECmk96a85EAIePvfWOWFWy/m/hy7QCD4LFp/5f9NNhuUETgijhI6uAJJw?=
 =?us-ascii?Q?Q7ffowh7ecgfcUViz6kasinW5X6DE5pYxXVKe9zZOFogU4MjsP02crWL6OUC?=
 =?us-ascii?Q?rSYxeu+WcHt0/eb3IRkCZ86uyzgSu7EG0L/rR2wpnbHaArmliyzlNVbSMoD4?=
 =?us-ascii?Q?WKXT+bMYf5W2jPEQy7rCWEBuGonCGkdYkizuVDVFQwoj6rm6ZLsWNLsRYlRM?=
 =?us-ascii?Q?sJ3t/vZc64sBSQH2EDOajZuS2011P3Wcjru242txK5lces8pI+aezS/jXv/V?=
 =?us-ascii?Q?D7BXy5Em1Dn9ak/6UdTk+o/ptitPTBfLOTOyJhYfE92H6n7qWiUhoyFUrpyH?=
 =?us-ascii?Q?yOKfOlMb3Hg6VMa3W1GIFFixuIWpcPMpLiAZESasqbhpcvVh69EQ25ew1Qod?=
 =?us-ascii?Q?mTlufHf4sVVbMvHM29STvfDAZ/BJ5EXGn1CpIojqsm4gk3CopofS79o0Yz+W?=
 =?us-ascii?Q?ZUcgLYKkXCo4reT0eGuVxMtYhiuP2CxdPS5V9cKZbYLpP/uXYbdTpUZzvSxK?=
 =?us-ascii?Q?qlTwRaQ1eMUl9VIybMa/SsICiFUBngElyuTM1RErN3WSNvW3JsZ0g8iDlQPB?=
 =?us-ascii?Q?aNNfuTyya9xARUEDUKOcXZFX7TUXrZ0tV2b/jLxyN/l2jM8mz5eki/ISYcsi?=
 =?us-ascii?Q?yEqiY15Pv6hk8An3kmqUx87SrlhIwcy3FC9MpuvcQCTnlVByqOKWEZdXAe7A?=
 =?us-ascii?Q?+sgE5YXYY6An8zITwA9AFreJXV8kNikQ4W/c0mX4j6D3ECSyKHksVTkMl/H1?=
 =?us-ascii?Q?crQHp7e6nu0ErfnceohqsoEVkENDO5+3W+c6BfatQ77FN0WWWrChVcis1wX9?=
 =?us-ascii?Q?hhdoCRnuVu3BYRNPGcrGdihmL3z6l9Wio3BuAR77uZq5fWW0UaiyG/zBtPKO?=
 =?us-ascii?Q?Kg8YdVNWC2x4rjBG965k/na9YStztOWhD8/wdL7U+Tr0/i5sFMNo75rrIn0r?=
 =?us-ascii?Q?G399gp86U6yH9SVmhdT/dFbfAUVO9HNa63S6NA=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: MN2PR09MB5785
X-OrganizationHeadersPreserved: MN2PR09MB5785.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT007.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(45080400002)(33656002)(450100002)(28085005)(34756004)(109986005)(19627405001)(7696
005)(9686003)(55016002)(5660300002)(6506007)(166002)(7416002)(26005)(8676002)(214804000
03)(52536014)(2940100002)(83080400001)(186003)(356005)(83380400001)(86362001)(8936002)(
1096003)(336012)(82310400002)(81166007);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 3e809327-6045-4bb4-6fd5-08d81cf6af72
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?C6AUae6Y5nXxCBjA0e4HhMg8ns5f1Q0YsGkt4zabDIQ+TLdM+gWTa3dB3hLe?=
 =?us-ascii?Q?G3PQggSWuEQ2TxIKtgPjTrAwoIiLKqaWfJZvFRyxSmIu4zBfBF0ghhxosYSH?=
 =?us-ascii?Q?fioCFRfK8QHTAaj0nsOPmxI61SoZxCJVA/elVn44/tGJeJ1KmknLDZs4jwXb?=
 =?us-ascii?Q?Cx/6Bt68V1JH1nx654YFuixRzPTwMNQQVZz+NX7XVTVvL/YLM+8rv+to9va6?=
 =?us-ascii?Q?JoHz50TrPlKx0pcykAS7LoBQB02CqW4D0Z4LBCHIGptNUVyJIIO60lgz4p1v?=
 =?us-ascii?Q?lmNuxhJgk5LaSY1iEzSJWEjeiwOu2EG0AOL/eIJMDfJT68Avo/d8I6/7oyRE?=
 =?us-ascii?Q?41bHu049DK2iAraqReVNyelsQ6WzuIge7iTy+sxg+Tw5L9Z3NMHwTRLljbKK?=
 =?us-ascii?Q?3sskNXxfBhlFBuhLbJYmU7HXW6U1xxxDYmdyFEbB1qeovpt3AqEI5vUiuQZF?=
 =?us-ascii?Q?jYjYL3TPvEl1A1/LxZmvKSt2JLpld7NPjJD/1yj9fTcg2Y0VGvo6OBmTPPGB?=
 =?us-ascii?Q?RQ9agIo6wVgHs3aDA9Yq3wzl0hyqjRqV4QcS16dnJ+QdTwNNG2XMO43YWjkO?=
 =?us-ascii?Q?aOTmgB9u9IVsMoIjTdLRsvDy/BHZeUobE/EJglw1NttGvrPVlIhClCDFGsRd?=
 =?us-ascii?Q?gLgglST5uWuGQkt/7Ex/bSbqqFiY1JhIeE1qSRyPs3UkwbufWG8DLXujY0cy?=
 =?us-ascii?Q?3AQ8J1NXvtJXRHDjv3eEVvZRIT0owIuEo0XZmcWBCBuG/3Yty5MdcvUbZa3i?=
```

```
 =?us-ascii?Q?aqz7t3wsX3aRYuQKyhap82BPEtCMFUa8Akk8xJDu+xiR+HmPZyXNaQwkJ6Mk?=
 =?us-ascii?Q?Q+26ldYPzattYlclA3m+VoF199HG33V2e+fVdxguD8DUz4gyBfY95SsqH8pY?=
 =?us-ascii?Q?XaAy/CAPrxzotBKIwrQREAoiAE7kKXJXnKudgt4qG1N79dD36Hk8PwJF37jN?=
 =?us-ascii?Q?CG1HVl5Vs5fehe9OKpA+xjXad2rLJ3hUax+xRTxALeSnw94r5wbq4MRv9e1J?=
 =?us-ascii?Q?nVm4tbkxZtJtw/Hdst8jhfJg1Q3YqBNN4OB01YXDpnddyRI=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: BY5PR09MB5777
X-OrganizationHeadersPreserved: BY5PR09MB5777.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT008.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(55016002)(9686003)(7416002)(86362001)(6506007)(45080400002)(336012)(1096003)(86760
02)(109986005)(8936002)(83380400001)(186003)(5660300002)(81166007)(34756004)(28085005)(
21480400003)(26005)(83080400001)(450100002)(166002)(7696005)(19627405001)(2940100002)(8
2310400002)(33656002)(52536014);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: aded0bf7-036d-4a19-2291-08d81cf6d94b
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?4Tj04mXPijq3TMGOUlHsyy9Q3Ih96furc96jZXTiVz4C8GdiGNwM6ZVyFkbJ?=
 =?us-ascii?Q?vtG3b7HBZZ+/4n+yuDCn7Nf87yXWJMkX78f2JHAU7LAmQXYx2KwuFhvXBpGR?=
 =?us-ascii?Q?F52/SNZISWR8orx10aW/lv+A5S1z7ILzPOcbwktXg+UYVWQKs9xf1gQ6ABUG?=
 =?us-ascii?Q?WIPj4WmzwwqGz0JO6rZBl0bFcO9BY2PxXFJMFD8OIWPFPcBZnuomirRTaRG+?=
 =?us-ascii?Q?eG5xtLSEE9PGxHE01DHDA963lRi5hSo5l/37zp0p0r8J7k/m+KW1SpidIwxU?=
 =?us-ascii?Q?bX8JnILqkKD1+478fKiub6M4RTRUNGJ1Sgvg7hV3G5fPbhtJ+IASpFaO3TYN?=
 =?us-ascii?Q?QS/Rdi8x0Lf0uuly4iRSyuOqjij/fxfI5ZXVZEtN1MtsP/AAfuinzUxzCfZo?=
 =?us-ascii?Q?e6IvYymXyuxUaUxlfOdu9oPH/eK1BTvaGpR4GvtY8UCE3O8cqX5ZLjX73cw3?=
 =?us-ascii?Q?MJG3hSniKBPVSJ3zbCiL5T66s/af0il7N2Nb91u7Am9gLxZcZx5Qb71bVuWU?=
 =?us-ascii?Q?9hsFyWbTyUW938623UGJaTxdGZEpGDysXoK5GdsQY37JUojb20WcmhueA6+G?=
 =?us-ascii?Q?I7l9qotM+LfT2Vm/37brmncpLIh6mp88rnzVDDrnEMr/rquQFfMEesOkJuEe?=
 =?us-ascii?Q?aoM8wkFRRAkUzl9OgfdaywT+eG1Y5yOzJVtn43+0Jh2t+k6LEbbQXTxhInQx?=
 =?us-ascii?Q?yEnPIT+k8U7JFcBBIZb9Q0gHSYyRr6VjI5gcEx9XoJR5aoa03VX7TAqRxnKZ?=
 =?us-ascii?Q?HTaQ90c3lRYAhOgQUgQClnrLfFx8qzSD/C7bh7ygx39AKUCmqxn5vG/t5tg1?=
 =?us-ascii?Q?NHE1AOkM63qwzK7aJUyjd6QObzjFtw8XfJwXzp/xPkyrJ4lGXebxya8yfkJS?=
 =?us-ascii?Q?dOEpaORUhFDUmeVZhfUIhd34zqjndY8wpu36ZTTA51UUcPfChCnmQhU9F8hC?=
 =?us-ascii?Q?aZF8vWOcq8XwioHZZkOvxy7EDOikMg7AGe82DGp9MV6em1dyqRbT9tT1wlWg?=
 =?us-ascii?Q?IVvMqpYXPX5p6uJ1OvJm+eY+7NQYpUOjRJ1WBng5kzcPYSA=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: DM6PR09MB4591
X-OrganizationHeadersPreserved: DM6PR09MB4591.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT005.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(19627405001)(336012)(109986005)(7696005)(34756004)(52536014)(8676002)(83380400001)
(28085005)(86362001)(186003)(6506007)(8936002)(1096003)(33656002)(45080400002)(21480400
003)(55016002)(9686003)(7416002)(450100002)(26005)(166002)(5660300002)(2940100002)(8116
6007)(82310400002)(83080400001);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 96e9d464-2a42-4459-8f47-08d81cf8fb66
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?fMbAx919U/T3ZXxXb/LFmjI2oyBXIxNL4TE1kznbHV88MgmpmTgrflqoV3dg?=
 =?us-ascii?Q?X3sp/DEiLzzyLVfJdLGDQPx8IQXqW0w6oRACbG6hlIkOSxSvTy4vUEjB3ly8?=
 =?us-ascii?Q?nHowU9e5LVQBwHm5AOhbrrZyxAglrH6QXljZXetPru39YXOFH3XVp0/6b0On?=
 =?us-ascii?Q?9ANCOGw05eolXysPHB/wgKBmpAjrN6Muy+k3ev1pU8W8sAHbd2C8b20PT20p?=
 =?us-ascii?Q?YDHIZrKnAL4p3TQNrl9oW8IMdvojDCqdaKXR9kizl5pTf0IIXYCsZH60hpDH?=
 =?us-ascii?Q?d11RhRYNzGNRYLW072T2THcoKNRJYI1+l7o44uSXEUm9lm9bUtdFEza+AZ6/?=
 =?us-ascii?Q?MMM9V0+HOm5TWidgDyPfMm9csPNsGhjkrgn2SZhTf42D7koLIlmz/afwxpcb?=
 =?us-ascii?Q?KfjHaUKv8jQhTnojigpINUiyr6Wf6VS1ZHAGh8juGEauN2ACBCuq7LWmzurR?=
 =?us-ascii?Q?sBbhLlLiXiw7W6K7FjLwdhwX557govmEV5M2J0kvrYf2CG778MvGDN/TcGmp?=
 =?us-ascii?Q?Pk5TX9p6DDaarnnaS3dFZRKH2L/O6/vohiVRnhkd9ICDlClgPZGr8HcJ5eQs?=
 =?us-ascii?Q?CKMPNJzZWads9tbKWqbaIpWMB2/Wq08Cb38UhAB7yVQUY0y+VfGmGwZpKH2r?=
 =?us-ascii?Q?DGCa3U+T8rpcPxD6MLtviT8QmGAXQC1wzJaDB70L3E0x4EaQ1Om5sH8U5fFc?=
```

```
 =?us-ascii?Q?Om/Sac+mS9DAMkfQWcnboTv0uxGY7L8TnjLpZ63Dm2lb6hJiXV4rdnd1WOkG?=
 =?us-ascii?Q?H+pmLd4vZOFkj+8LMLvTWgAyzGypDM8haWrI98x2RQlK0yuLjO+F0j78J8wX?=
 =?us-ascii?Q?8ik8pMas7p2MaHrWA9q2URG6+jOCnBqUw7nezqf7V2/TeTB8RKUrP8pHr1ni?=
 =?us-ascii?Q?rbCkzTlhpXcGAQTt8QtZu4RTD8a1hVGVGaRAk7SwQf9o1VpCOLgZ35HD7F5H?=
 =?us-ascii?Q?Cz4nNPQKlgws49trP8ve89TpTR/F6BsaRuaVp4KiM2AmbnCJOoiJ/0LGlSdQ?=
 =?us-ascii?Q?JhlvCsDpRQxaFVwlsGI0gc/M9NOP9BCp/GsM0wmfiRH43L0=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: DM6PR09MB4838
X-OrganizationHeadersPreserved: DM6PR09MB4838.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: CY1GCC01FT010.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(166002)(6506007)(1096003)(5660300002)(8936002)(26005)(186003)(82310400002)(4501000
02)(83380400001)(336012)(7696005)(21480400003)(7416002)(356005)(55016002)(45080400002)(
109986005)(86362001)(28085005)(33656002)(83080400001)(9686003)(8676002)(2940100002)(525
36014)(34756004)(81166007)(19627405001);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 46a6ab41-98fe-4465-7a07-08d81cfb17cc
X-Microsoft-Antispam: BCL:0;
X-Microsoft-Antispam-Message-Info: =?Windows-
1252?Q?YKGNe4qFcHE+oGW9G+lkdGIEgOIKD+eI95kCWPame+JrrUaXZZvgFoW0?=
 =?Windows-1252?Q?LMwkzttOv//9y9BqCzlleKX6wsNFiL5FXbbzOdIYok6LDRWR4H6upLKU?=
 =?Windows-1252?Q?Q+3VOM86kR1sFSK1bPNic+q1uZPFCFiezDmknwvATEoP16LOPVRkO0Ni?=
 =?Windows-1252?Q?BtW0EE1kirXADpA9JVQqLuS/JlnVI1sFpVY80tYZa13DvmbUVZ4GRqAl?=
 =?Windows-1252?Q?6r7X4CGI+XfB2AVUNozJY1e+v1fQIMWrYy7yHuKYZ2RZT7+A02TInqoJ?=
 =?Windows-1252?Q?mxGwj5PMdlk4syrhqo/c2Gv1dLWIpux/L4FUIzldT+Rw1HCg1k9vC8sn?=
 =?Windows-1252?Q?NzPmhWEvVBZVRVcCIcY7hm3N7c4EEI/Lt5M+0abxv/t67EE4FtbxxR+Y?=
 =?Windows-1252?Q?4OpulGL3YwqQEyZYdJQpf19aPoIU/wQWqHIzVh5FlUWYiqYYT9AQUriN?=
 =?Windows-1252?Q?Gg+qHuKDhPWs72f3zNYMqmq2sN0YpsFPupL0xOuvSF5rNr1ms06h8uBo?=
 =?Windows-1252?Q?6wawt6o/PNsapivPicTKU3592I23tl/maQPdsra592qAXT9OW8GyaRnm?=
 =?Windows-1252?Q?hZDWADE9lhLL87VgBLQtEoL+dXh6hZ+KAD2/zDzEBaKtuHauHUm3OP1c?=
 =?Windows-1252?Q?nfJH6HhNEfVd1BN9/H40fS15i+wHoJoGj7ee64n4YvxE7HK84l+7F/Mp?=
 =?Windows-1252?Q?cfZ10QznBCvuIfmiLx/AjyWoz4XclOJdufrY8dkuIUyPVyvZpGkfNU1m?=
 =?Windows-1252?Q?cJsPimfDB143olkzXqkmJaff/7t0WA2i8yINGV3KhdRWxJG0ccucQ17N?=
 =?Windows-1252?Q?auQtze/Sz+tD6QNDEQxEFRnuFnD99tHVJH8P3pULPVszGziUUOTMCGo4?=
 =?Windows-1252?Q?1ttbggxHFGy1gn1F+eBrEx8DDkEngK6jCQPLS/PPwQT+ZLCZo+6+uG4I?=
 =?Windows-1252?Q?ORKOcQmyZX6Qr1M8zC5dK5Pfpa+2G6K0OJDiN06m8Zyyo4MzixfPMKMm?=
 =?Windows-1252?Q?4oa1x47OiurBzlItUf0d/xiVBABLzUmDy/VomBEw0ZYQZEhDqXud1CV9?=
 =?Windows-1252?Q?UMDUvG1kWkSuotsei08u0vH9/LRKVEnTr+3IJ0s1FBQteJg3K/OgyVMA?=
 =?Windows-1252?Q?+TOCvl7Kw8h2Zj1e716Jgssl7Akp35Fp0fS2NWgFJk87VPoA8QkHVRlf?=
 =?Windows-1252?Q?1XRrTCuQtoueo1kM4jgsbD/0OLRPA+zExjAXau8M1cIB9X1lADJy6hfG?=
 =?Windows-1252?Q?/IMiyptXL1HvMHMmmGfnm8AvlTVTHVlLWdQTg+HO8ugaTd9WCQfu+MTB?=
 =?Windows-1252?Q?frIArg=3D=3D?=
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 30 Jun 2020 13:40:38.4698
 (UTC)
X-MS-Exchange-CrossTenant-Network-Message-Id: d60cf752-ee33-4157-39fc-08d81cfb2cb5
X-MS-Exchange-CrossTenant-Id: 8b4d55ae-6db4-4e05-a85c-59d6a256cd6e
X-MS-Exchange-CrossTenant-OriginalAttributedTenantConnectingIp: TenantId=8b4d55ae-6db4-
4e05-a85c-59d6a256cd6e;Ip=[162.217.184.79];Helo=[CCCASV01.CCOUNTY.com]
X-MS-Exchange-CrossTenant-AuthSource: CY1GCC01FT010.eop-
gcc01.prod.protection.outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Anonymous
X-MS-Exchange-CrossTenant-FromEntityHeader: HybridOnPrem
X-MS-Exchange-Transport-CrossTenantHeadersStamped: DM6PR09MB4936
X-OrganizationHeadersPreserved: DM6PR09MB4936.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredByDsnGenerator: CCCASV02.CCOUNTY.com
```

Undeliverable: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	Microsoft Outlook <MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@cookcountyil.gov>
To:	CCSO.INTEL@cookcountyil.gov, Mary.Tamme@cookcountyil.gov, Wanda.Barnes@cookcountyil.gov, Vincent.Gamez@cookcountyil.gov, Thomas.Shader@cookcountyil.gov, Tangenise.Porter@cookcountyil.gov, Tamara.Levickas@cookcountyil.gov, Samuel.Cory@cookcountyil.gov, Ronald.Prohaska@cookcountyil.gov, Roger.Comer@cookcountyil.gov, Robert.Waller@cookcountyil.gov, Robert.O'Neill@cookcountyil.gov, Richard.Petersen@cookcountyil.gov, Rex.Knaperek@cookcountyil.gov, Paul.Riley@cookcountyil.gov, Paul.Huss@cookcountyil.gov, Nancy.Pavelka@cookcountyil.gov, Michael.Quan@cookcountyil.gov, Michael.Gomez@cookcountyil.gov, Michael.Anton@cookcountyil.gov, Maurice.Cernick@cookcountyil.gov, Matthew.Walsh@cookcountyil.gov
Sent:	June 30, 2020 8:55:43 AM CDT
Received:	June 30, 2020 8:55:48 AM CDT
Attachments:	Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

Delivery has failed to these recipients or groups:

Mary.Tamme@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Wanda.Barnes@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Vincent.Gamez@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Thomas.Shader@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Tangenise.Porter@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Tamara.Levickas@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Samuel.Cory@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Ronald.Prohaska@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Roger.Comer@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Robert.Waller@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Robert.O'Neill@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Richard.Petersen@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Rex.Knaperek@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Paul.Riley@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Paul.Huss@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Nancy.Pavelka@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Michael.Quan@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Michael.Gomez@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Michael.Anton@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing

configuration or mailbox rule setting. If the problem continues, contact your email admin.

Maurice.Cernick@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

Matthew.Walsh@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

The following organization rejected your message: CY1GCC01FT007.mail.protection.outlook.com.

Diagnostic information for administrators:

Generating server: CCCASV02.CCOUNTY.com

Mary.Tamme@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Wanda.Barnes@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Vincent.Gamez@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Thomas.Shader@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Tangenise.Porter@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Tamara.Levickas@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Samuel.Cory@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Ronald.Prohaska@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Roger.Comer@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Robert.Waller@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Robert.O'Neill@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Richard.Petersen@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Rex.Knaperek@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Paul.Riley@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Paul.Huss@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Nancy.Pavelka@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Michael.Quan@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Michael.Gomez@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Michael.Anton@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Maurice.Cernick@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Matthew.Walsh@cookcountyil.gov
CY1GCC01FT007.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT007.eop-gcc01.prod.protection.outlook.com]'

Original message headers:

```
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
 (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
 2020 08:40:40 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
 by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:40:40 -0500
Received: from DM6PR09CA0036.namprd09.prod.outlook.com (2603:10b6:5:160::49)
 by MN2PR09MB4843.namprd09.prod.outlook.com (2603:10b6:208:21b::22) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20; Tue, 30 Jun
 2020 13:40:38 +0000
Received: from CY1GCC01FT010.eop-gcc01.prod.protection.outlook.com
 (2a01:111:f400:7d02::208) by DM6PR09CA0036.outlook.office365.com
 (2603:10b6:5:160::49) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend
 Transport; Tue, 30 Jun 2020 13:40:38 +0000
Authentication-Results: spf=softfail (sender IP is 162.217.184.79)
 smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
 header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
 CY1GCC01FT010.mail.protection.outlook.com (10.97.0.149) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:40:37 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
 (10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
 2020 08:40:05 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
 by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:40:05 -0500
Received: from MWHPR09CA0045.namprd09.prod.outlook.com (2603:10b6:300:6d::31)
 by CH2PR09MB4588.namprd09.prod.outlook.com (2603:10b6:610:65::13) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
 2020 13:40:03 +0000
Received: from DM2GCC01FT005.eop-gcc01.prod.protection.outlook.com
 (2a01:111:f400:7d01::201) by MWHPR09CA0045.outlook.office365.com
 (2603:10b6:300:6d::31) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend
 Transport; Tue, 30 Jun 2020 13:40:02 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
 smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
 header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by
 DM2GCC01FT005.mail.protection.outlook.com (10.97.3.0) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:40:02 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
 (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
 2020 08:24:57 -0500
```

Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250)
 by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:24:57 -0500
Received: from BN6PR09CA0050.namprd09.prod.outlook.com (2603:10b6:404:7a::12)
 by SA9PR09MB4638.namprd09.prod.outlook.com (2603:10b6:806:4f::10) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
 2020 13:24:52 +0000
Received: from DM2GCC01FT008.eop-gcc01.prod.protection.outlook.com
 (2a01:111:f400:7d01::207) by BN6PR09CA0050.outlook.office365.com
 (2603:10b6:404:7a::12) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
 Transport; Tue, 30 Jun 2020 13:24:52 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
 smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
 header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by
 DM2GCC01FT008.mail.protection.outlook.com (10.97.3.193) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:24:51 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
 (10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
 2020 08:09:46 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
 by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:09:46 -0500
Received: from CY4PR09CA0093.namprd09.prod.outlook.com (2603:10b6:903:c7::31)
 by MN2PR09MB5515.namprd09.prod.outlook.com (2603:10b6:208:211::20) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20; Tue, 30 Jun
 2020 13:09:44 +0000
Received: from DM2GCC01FT007.eop-gcc01.prod.protection.outlook.com
 (2a01:111:f400:7d01::200) by CY4PR09CA0093.outlook.office365.com
 (2603:10b6:903:c7::31) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.23 via Frontend
 Transport; Tue, 30 Jun 2020 13:09:44 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
 smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
 header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
 DM2GCC01FT007.mail.protection.outlook.com (10.97.3.159) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:09:44 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
 (10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
 2020 08:08:44 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
 by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:44 -0500
Received: from CY4PR09CA0074.namprd09.prod.outlook.com (2603:10b6:903:c7::12)
 by MW2PR0901MB3819.namprd09.prod.outlook.com (2603:10b6:302:6::17) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.24; Tue, 30 Jun
 2020 13:08:36 +0000
Received: from DM2GCC01FT007.eop-gcc01.prod.protection.outlook.com
 (2a01:111:f400:7d01::201) by CY4PR09CA0074.outlook.office365.com

(2603:10b6:903:c7::12) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
Transport; Tue, 30 Jun 2020 13:08:34 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT007.mail.protection.outlook.com (10.97.3.159) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:34 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:08:33 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:32 -0500
Received: from BL2PR09CA0034.namprd09.prod.outlook.com
(2a01:111:e400:c743::44) by BY5PR09MB5969.namprd09.prod.outlook.com
(2603:10b6:a03:24f::15) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.23; Tue, 30 Jun
2020 13:08:30 +0000
Received: from DM2GCC01FT005.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::207) by BL2PR09CA0034.outlook.office365.com
(2a01:111:e400:c743::44) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend
Transport; Tue, 30 Jun 2020 13:08:29 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT005.mail.protection.outlook.com (10.97.3.0) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:29 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:08:19 -0500
Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:19 -0500
Received: from BL0PR0901CA0023.namprd09.prod.outlook.com
(2603:10b6:208:1c0::33) by BYAPR09MB3126.namprd09.prod.outlook.com
(2603:10b6:a03:9a::14) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.24; Tue, 30 Jun
2020 13:08:17 +0000
Received: from DM2GCC01FT006.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::202) by BL0PR0901CA0023.outlook.office365.com
(2603:10b6:208:1c0::33) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend
Transport; Tue, 30 Jun 2020 13:08:16 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT006.mail.protection.outlook.com (10.97.3.107) with Microsoft SMTP

Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:16 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:08:12 -0500
Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:12 -0500
Received: from BN3PR09CA0059.namprd09.prod.outlook.com (2603:10b6:400:3::27)
by BYAPR09MB3237.namprd09.prod.outlook.com (2603:10b6:a03:a2::22) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.24; Tue, 30 Jun
2020 13:08:10 +0000
Received: from DM2GCC01FT009.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::204) by BN3PR09CA0059.outlook.office365.com
(2603:10b6:400:3::27) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
Transport; Tue, 30 Jun 2020 13:08:10 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT009.mail.protection.outlook.com (10.97.2.68) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:09 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
(10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:07:51 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:07:51 -0500
Received: from CH2PR09MB4491.namprd09.prod.outlook.com (2603:10b6:610:36::19)
by CH2PR09MB4395.namprd09.prod.outlook.com (2603:10b6:610:6d::18) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
2020 13:07:47 +0000
Received: from CH2PR09MB4491.namprd09.prod.outlook.com
([fe80::54b4:1a30:151b:810f]) by CH2PR09MB4491.namprd09.prod.outlook.com
([fe80::54b4:1a30:151b:810f%5]) with mapi id 15.20.3131.027; Tue, 30 Jun 2020
13:07:47 +0000
From: "CCSO Intel (Sheriff)" <CCSO.INTEL@cookcountyil.gov>
Subject: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement
Data
Thread-Topic: Pass Through - (U//FOUO) Criminal Hackers Target US Law
Enforcement Data
Thread-Index: AdZOUZRVrVUDcfOlTiiWh3YE0iFXiAAjZyaaAAALg8I=
Date: Tue, 30 Jun 2020 13:07:45 +0000
Message-ID:
<CH2PR09MB44919AB3DDCF48A1DC9A721BF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>
References: <LYRIS-103909956-1411846-2020.06.29-15.13.38--isp-les-
north#lists.illinois.gov@lists.illinois.gov>,<CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH
2PR09MB4491.namprd09.prod.outlook.com>
In-Reply-To:
<CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Authentication-Results-Original: cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=none action=none

```
 header.from=cookcountyil.gov;
x-originating-ip: [162.217.184.194]
x-ms-publictraffictype: Email
X-MS-Office365-Filtering-HT: Tenant
X-MS-Office365-Filtering-Correlation-Id: 4e80628d-db46-4c13-8d96-08d81cfb2c49
x-ms-traffictypediagnostic:
CH2PR09MB4395:|BYAPR09MB3237:|BYAPR09MB3126:|BY5PR09MB5969:|MW2PR0901MB3819:|MN2PR09MB5
515:|SA9PR09MB4638:|CH2PR09MB4588:|MN2PR09MB4843:
x-ms-oob-tlc-oobclassifiers:
OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original:
dorE26jV2iSCAAZPeOVhoLD94Hv4kxz7P8odY90Qx9txS684fFRvsQrQNNuMcw5j3CXAvxwJ6RKVNhma4waBTSV
NDGxp/cmBk4EE1mmOJLigUqP/p5XBKfbHvh7l8XKcuXNUZElkV+zSCD0eo8miajinOJW7JVM+LKl83OPl/aGzKO
q6bOCroeq1axlnk4eWaDTHoAOIyh54/JAVk4Vrimq/BMjI4mSCAvqOgQu1CSA3SG/epzZtTashTb6dRWMQgeo+r
JRKNCeaiFc3HMFzVIRVpFATyE6RE6OVqdVOG2K5PsnuO/NhyqisQzWRtPZnKnQE65W6iRiiEbtgObqS5ZzmjcRR
H4CGvuJFl3tG1yM=
X-Forefront-Antispam-Report-Untrusted: CIP:255.255.255.255;CTRY:;LANG:en;SCL:-
1;SRV:;IPV:NLI;SFV:SKI;H:CH2PR09MB4491.namprd09.prod.outlook.com;PTR:;CAT:NONE;SFTY:;SF
S:;DIR:INB;SFP:;
x-ms-exchange-antispam-messagedata:
lfyUdUNo6Rf5kP/RudyGbEyoz+NqqBXdgwdrJdYqEl4KGO77nPkGtTCiHAy0fTDHpKfau4FlsKcP4NPTjBZt0qo
M0swESqf76XMqi53/H/ftP7B223MsFZ9fg5VOxHvc32BClwGPDW+JR3i1qP6YkWVZTuxClUHYV/m3qO/WA7zFrn
q1HGYz/BQ9xQPFzN9ySyJCGd+j9svK3rmnh7njYATQdwBhm/L/06zYHtkcQuXCphogmV5EwxhUeYsDQ18Z9Lphi
UGfntO4ZLeJKhaQlTC86oFyonuAQ8DSt4ZyaYeVXcbNOuyrBFtWcyDVzIMi6RwmDU4aA8eX2yeHjnQ1ngAXfb6w
xmTfCdhMIo3Kbla8ErnlLS56npY6/GW/CGnf1qCGoLMKgNMBwrDrq0yAnvMuo6sEXA/bdkPEDSJD8JxHzl3yOp7
4YkgohRwqBYld6GvNdDvRPJe12IzDacv+MFwLljmdkuIxYJEykmLdGp8GhPL73qvrmFbfbAye08sP
x-ms-exchange-transport-forked: True
Content-Type: multipart/mixed;
      boundary="_004_CH2PR09MB44919AB3DDCF48A1DC9A721BF56F0CH2PR09MB4491namp_"
MIME-Version: 1.0
X-MS-Exchange-Transport-CrossTenantHeadersStamped: CH2PR09MB4395
X-OrganizationHeadersPreserved: CH2PR09MB4395.namprd09.prod.outlook.com
To: Undisclosed recipients:;
Return-Path: CCSO.INTEL@cookcountyil.gov
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-EOPAttributedMessage: 7
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT009.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(2940100002)(34756004)(356005)(186003)(86362001)(109986005)(166002)(33656002)(82310
400002)(336012)(28085005)(6506007)(26005)(45080400002)(5660300002)(450100002)(9686003)(
83380400001)(21480400003)(81166007)(7696005)(83080400001)(7416002)(55016002)(1962740500
1)(52536014)(1096003)(8676002)(8936002);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 2b67f42c-4bba-4f30-216e-08d81cf695c1
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?2YnnqSlRMKSaQYOuMk4UvXH9r7tmUHgfrEZ3E/GUi6pKQO11IbyJqgyrsLZd?=
 =?us-ascii?Q?78Cg9LxJLN+Bnf3NxRLRTj8JOg3VAsyCJNaER0hoFEfHX9fpkdaPrlMx+mJ1?=
 =?us-ascii?Q?e9MpnKYW8PhlNs067dxgePaRIYe2c6kZmYRpeZoeAY1JcAduS1keyRBSyG0a?=
 =?us-ascii?Q?a2SMxC+3UeFElmkgQCPNIFPzGqL8YfqQxCQ7vllHCfq5O4tHR2e7NinAyJNm?=
 =?us-ascii?Q?o5T2B5LWn0VsaDR4//C2Q+ZmM8uP2gOT5IY5LQneJ4vOj7KYkHv5o+/i/Pht?=
 =?us-ascii?Q?FLeLiML+TU2bvQ9jD5kxUlzn0uss41dj3ZwhFkNv97LDURqrFNrakPXn+vRI?=
 =?us-ascii?Q?AIhKOjN6GIrjTtSaG/KOm/2j0RUaAPHeF7H+F/2fJHV5/lbBFS9Yug7sUTap?=
 =?us-ascii?Q?dQ28QVEcm2n6NClEf0uWTM9sSqnA1dhyDUTmAKaNXqSjfSuMQXHHw+wF33xC?=
 =?us-ascii?Q?QIdypmtG/Y9+HoMevu+6Vb5XStpEgNTQaxsKsOo28jjrT/A2jHtTpTDo7u6R?=
 =?us-ascii?Q?5iWPFJzMlC6AM3HX/V/AC7+XIMgJ6a+MsnqeEDNaaLn2UiQybRL1yunCBgYu?=
 =?us-ascii?Q?wxDgTqEPFmZ6BjSESEfnKOmm0J3CmfrGpdscVRA7GzoZDWYRIDnqEycxlObB?=
 =?us-ascii?Q?20SrmGlSNQyWQbRXmuLJAAu9D1JTieldSmeG4NJ6zmykilSpsUi5A1dxm3xP?=
 =?us-ascii?Q?Y0HfA5Rk6q9+4V/4XlY64zNaVhlOMJMa4TtDNUJ7icLGUvhj3lvP+f/4uB+d?=
 =?us-ascii?Q?7c0vFh7Z/eESfDs71i8irgvhgGRredGN4lVFxOuEem5sXl3aDYN3FTvfAEA4?=
 =?us-ascii?Q?enh15qt5uFYEtA1/T67zatpvYIM1rUiIKP8GRKzR7f/ds6mx2bAXhLxJw4el?=
 =?us-ascii?Q?qraJZXLpOpmYhoINtYOaE+8NhX/KwAtosS45EUlWgKn5m3fXtqndxXSwUpKy?=
 =?us-ascii?Q?WIVb1Vm0Pv7ubMo9UNiXx/e13PBnPmC4+jaLYaijWeElu0JEG0D7VYbmGeM6?=
```

```
 =?us-ascii?Q?MSR8yx6VDgzgxbRvbPI6FhyPi08rCQwQDXDdEMf5ApBiWyS0lFgo1DXxndBv?=
 =?us-ascii?Q?HOm2/+Zb7L/VtZiJ9b5vCfi2h/z7SVelYUWv1XukSt1kxlyHHtndqy5QLLLW?=
 =?us-ascii?Q?ZgSEEAQgF6N1Te950zuGiogczb666+YXa4S0pfvOzhCcJxSMUq+MUAUCwnSP?=
 =?us-ascii?Q?LRUg8iUK6CqnJ2XplILi9cZW7vn+GsRcTcMUnEKru4k6qx1GT6leqk4OrdB3?=
 =?us-ascii?Q?eCUsY9NONBaJgjnjsYj6?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: BYAPR09MB3237
X-OrganizationHeadersPreserved: BYAPR09MB3237.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT006.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(19627405001)(8676002)(2940100002)(1096003)(5660300002)(55016002)(109986005)(893600
2)(86362001)(34756004)(83380400001)(9686003)(7416002)(450100002)(28085005)(52536014)(45
080400002)(186003)(336012)(166002)(83080400001)(82310400002)(81166007)(33656002)(26005)
(7696005)(21480400003)(6506007);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: b2a1b3c9-afa1-464b-f65e-08d81cf6a335
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?vacDUPMnBNFqkjDGp1XhwU0lK8Z6qtPwuCMY8lJbunFBrhMvok2FcDnGjwvE?=
 =?us-ascii?Q?lG3mABVb3kAutKMio6t3Su61vFUJN7QR9+UN8Mf8CD7+t+amh2IaulHXdtMT?=
 =?us-ascii?Q?m9wvRVeUoKQSrG6AgHzSZYAM+IvrljQYxbtRQijUMLRxK1TTFk/icWpNhEQz?=
 =?us-ascii?Q?fASB9fi1RzzJWEN8oeGE0bMO2PkokfBCiuGjqj5YIRb7MCLV26OZldjr3Dnu?=
 =?us-ascii?Q?smLjQK8p2Q98f86S8o8f6qICPhNGakVgTP0Q0VsvazQ/oRYW11RxavvVF4pR?=
 =?us-ascii?Q?z18A7TQQ/kdBZkiPIO+eRbK4S1zmlVCahjLxPd5U7K12eyMUYIuh/yvNDG8S?=
 =?us-ascii?Q?hPNmuwQ6MD8o4FxwcXmM0gzyjbE0doEWedeoa7gKfcbpgceC3ikcb8Ak5PCv?=
 =?us-ascii?Q?CtDqVHpCTko4fvxQOGHXol2qFM6x3mf6MpEps6eyjCzorIsZJJQ9LmW5VBQV?=
 =?us-ascii?Q?wzTMUWpWdNAMepU9IExlixad97ah2+fEaPOZxddzE6sTqBsfyvVILV6JuqC2?=
 =?us-ascii?Q?f5faczjciITOgKHkzL71YkFzESJHrBUukKpKHjiB+Xu4y6Zacxk7F2ItHVnC?=
 =?us-ascii?Q?W2dfzeFINMvxXMlZajG+o/HgL4TWoJnMg7fk3/5irs7zYDgsUu2kt5zfd3fk?=
 =?us-ascii?Q?IyWAMOC+mqYNAl32M0TCdPizuB0CeOvGcmYNf+90oAVMXuuboDeaSfzUMFaf?=
 =?us-ascii?Q?S4om39vx9lroNxhvX0E6q3bEYr310+QE3hYzbchG6HkAyVmtlIY0HuPEhToB?=
 =?us-ascii?Q?evfO305CBojelR5bGgZH7azYNtf4q3hh7Rncv+mXlWeJ7ufa351p4OjFQZe6?=
 =?us-ascii?Q?lFJOSwvQgcnCbh7y0sC7Y9aXViz9w6A/aMz/qHTLV5djDUGvKR5SpN3deR7j?=
 =?us-ascii?Q?kvGdIqtglIICGYJ2XgngCZCLDc19f6jWAOF39zNlMDtjttmm9Wz1862A2haa?=
 =?us-ascii?Q?Vw2t91pIIKeGe1sNDazwIKOQtndZVKRjfqUg2y/NALjJl8M8mDa01b9dBmfY?=
 =?us-ascii?Q?1YDhb87yqbbVGI8RQNNzRJ62ITKM9zPveIv6aB9Qm7P3XnY/UJjBv4fQN9Eg?=
 =?us-ascii?Q?LtuzdclWEqaxpvV2vQJts5wqyv8URekMYFNm+FGdM+DGrz8EXvVZxfVxeeBy?=
 =?us-ascii?Q?pWjrvBTtWTTsB0QLsa/SqD98CqwIiaREBK/qx1kJX4DKcuyPBC+d+0EpNCkh?=
 =?us-ascii?Q?DdiA8/vB0Ub0DOduO6283cLip62fsbaXDwMn7A=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: BYAPR09MB3126
X-OrganizationHeadersPreserved: BYAPR09MB3126.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT005.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(186003)(26005)(6506007)(28085005)(34756004)(7696005)(336012)(7416002)(2940100002)(
21480400003)(8676002)(8936002)(1096003)(45080400002)(82310400002)(5660300002)(166002)(8
6362001)(19627405001)(83380400001)(55016002)(33656002)(450100002)(9686003)(52536014)(10
9986005)(81166007)(83080400001);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 0472d190-725c-4fa2-7033-08d81cf6a757
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?H7j3d3akoUwDy0X2s6yWLOxFnSAY0KF329OWQHrI3p/d8mEYG8zv0/kiQM8V?=
 =?us-ascii?Q?MkinVrHYN6IzhfgJK8NzVkcDiZGhdwwmbIQhifU7J6RUwpWOlpPxGgPKR6vm?=
 =?us-ascii?Q?mIbrYEQbV7L/cRlggoEkG+DoQIFIJSiunW7OqK0QxK8FTFdzqTQuFKUdW8CB?=
 =?us-ascii?Q?6AmBjbOIiw8DWDnh5+MD96E+GaIeID2ZScqHY7WR8Fwc8dwnqK+AR2mhcKSC?=
 =?us-ascii?Q?c78Qs9VfCX3ze43lMdCtE7/XSwJLM7mgUvx0v/Pa0PKuXm0Eb0h7YTOcybnN?=
 =?us-ascii?Q?R524x62b6a+eWznIZCc890xsvYFb/kAVF3oLDaN59omqYOZTzfsnJQF+bR2V?=
 =?us-ascii?Q?FNdn3jc9wz4E6DFrWg/VyWm6OikSkZYid9mbDSPNm3KddRq4seey7DlCJ+f9?=
 =?us-ascii?Q?hJT/zIEZkcUP9WlDiXFVocLUFbL/EKFGtCq/0S6JEbIdoJLnThSeta6DSmAW?=
 =?us-ascii?Q?beAVv3PuJs7Ll/RfqPhNMjc2ZNp3q1uhf1uVHPec5cmvwN3NfGn6cueg9e9h?=
```

```
 =?us-ascii?Q?UGcwxLdB3QJBRyx7PCjdb29FCkbvKrdJry1x5sHmmfyHVAnhQyNeSsL2lGfy?=
 =?us-ascii?Q?t4ttIJ9wuwffHuhIpkMpdnKj/Bz3EiGTmNrNsSDkmIQJ9SiMa1+jtxdKIyqd?=
 =?us-ascii?Q?/70jZrJNViO2io4pWwQKEVbRH+OSI6hjuMo2irpTQejsc8oZfpSIWM+OvEfZ?=
 =?us-ascii?Q?mxRhlNl/ZNh8EEe0jW9561tNkn9RbI3Bb6drGAdNo/C+0hjG66wgKyqtew2N?=
 =?us-ascii?Q?KiZUUrm5wIglIBHHxxhgJ4Qkq/u4nohfXIvd9gtMIHwO5etyz1yJW6DnYAuo?=
 =?us-ascii?Q?DHG7+d5grPzZ8XhKkY2CAb3fmzUSo4IWMqILtWaPTdXbw/nLC4YswidYGm8y?=
 =?us-ascii?Q?uyaFliF2IxbWPDiB3TQzUxzm4fjaslun50haCfZFq/D8WDZprmRgq+wUKxBV?=
 =?us-ascii?Q?E5oOGJ7akfjRcwMUtAiRILJvMG/uICFrd1kj2CS9qY03Ie9g7oyR1ZqS2nMh?=
 =?us-ascii?Q?nKrXt4PRR4V98IKrGrmMBQxGfCxsy0LKt6Se0mWo8JbTReA=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: BY5PR09MB5969
X-OrganizationHeadersPreserved: BY5PR09MB5969.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT007.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(7696005)(81166007)(7416002)(9686003)(83080400001)(450100002)(21480400003)(83380400
001)(52536014)(8936002)(19627405001)(1096003)(8676002)(55016002)(34756004)(186003)(2940
100002)(86362001)(28085005)(26005)(6506007)(45080400002)(5660300002)(33656002)(10998600
5)(166002)(82310400002)(336012);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 6656c69f-ce4e-458b-a825-08d81cf6aed5
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?KyeCcyPsiXfJHcTkhqbntrzp7OZ/K5AvKppenGFhy/9FEYnV8ZEv7QxnXZY6?=
 =?us-ascii?Q?bOzW7Axfi6cS81zUdfTCXjCS9C3SHaYipA5x8+4+HD8rXGFjB3MjFtJxUTai?=
 =?us-ascii?Q?RVNM0/UxZ0Q0cfQ5U0f+O3H8MpL+9VmiZrRYDOZu5ZptAKycGwVSbgInn5Nz?=
 =?us-ascii?Q?NoQMrqMZJPNp82c1mc9a0O0jjFvR/ucEbr4/EUOcE6VXsFOtYgbc5eBYcBaz?=
 =?us-ascii?Q?6waq3lxWZjOPSYmMEZHn2QjB9iK7q6fCPU1Wvf99s31F5PvZh8sJzDg6rq5t?=
 =?us-ascii?Q?4ML/CuHv383cYLnNVrmFAfGd6Q5NxDKwnkM55lZFYeD4++UQ4mMACBO3UK5+?=
 =?us-ascii?Q?lt9vT82TG3mrv7ATbE+4hu/fLc5+bm7LHC7yDr3MkB89hkXpvEGCn4Hsptxn?=
 =?us-ascii?Q?Fv5ClgYAty2+sHkEiUvqFJBNefpZid5CHYOXmIgsklJKnkIvIVRteZiR93n6?=
 =?us-ascii?Q?mp5sA4fX9rL0Xf+z8cS3VkgrNggsBKcKf49SMVtjgI7XZ/7uVgswLkfuxEWl?=
 =?us-ascii?Q?elud5icFf5gFdjFYbViFK/C55kXuKnSUYtCxYXTsCGIAhBmIhRaKfd1nNI5d?=
 =?us-ascii?Q?YxwwJyCqQ7/V3KKkoFy7EYrMAwUm9bQJSSrM3Iy/wU5jkwUsR9jZOPibhUdi?=
 =?us-ascii?Q?pDhbszCcvFVCVJ8pqXLZ0l0fyqcl/VlMNs5G65xAngRS96vuBpRYSokcRAkQ?=
 =?us-ascii?Q?pSBqQC8pw9W7MYneCfZwu4PN2wkVkFjIQdkdO4PCEpu4rzoHL9uZsBrUPoIJ?=
 =?us-ascii?Q?WLkJU4JsF6Kz6PGSSBHHZqn5JlgK7qt63C00UTIoVeXQ39ZO4WcUTs3hR3B6?=
 =?us-ascii?Q?xwo5nJHuZGh11U9CseKph5Gmfq9v41WTrsuRjO5GwSmJdMjf/jBiemHlZpgN?=
 =?us-ascii?Q?tI227AsieNDUxsgI+RHHeZEsLOcsm795/TEwRQjca9DtK3q61npYpx2s4YDd?=
 =?us-ascii?Q?RnNjm5vboOcWC8F9U8WfLNj6jAcGkosyDuUJK4JCCVINXKK9C521sqr8NQT0?=
 =?us-ascii?Q?siJgbDNwf55SjVr26Q9nWI/XC/ohGQirn9UDEQZh+G/GL7ODnDAqteQnQMjo?=
 =?us-ascii?Q?vK7QIocozmaQDesTjSZPRjebQ2GJA6EY10MXq+D+cb8e7zJvvaEpfs6tGmPy?=
 =?us-ascii?Q?RfnT6GWRM4SbA7wunxafHcJMDPvOoFaj0Fcws0K8KL5l1ol0c+3fMT0ChcSx?=
 =?us-ascii?Q?UoC3NvS5/viOBsQ4dkOlvlqgELjDMJxPY84HkQ=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: MW2PR0901MB3819
X-OrganizationHeadersPreserved: MW2PR0901MB3819.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT007.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(7416002)(45080400002)(450100002)(83380400001)(8676002)(336012)(33656002)(7696005)(
83080400001)(166002)(82310400002)(109986005)(81166007)(9686003)(52536014)(55016002)(260
05)(2940100002)(8936002)(1096003)(186003)(86362001)(5660300002)(21480400003)(1962740500
1)(6506007)(34756004)(28085005);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: fb4d3d08-2852-4452-d783-08d81cf6b1ef
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?mOheSDvPyw1VKc3YLS33roidKXU4McbXS8FL6Oc8kyQfNhRJgAm0K718hYu/?=
 =?us-ascii?Q?hNdGPUecQcwBA7Ww/fChXRb0vXaPnzcf/ThhbuFgkOkZdodcfoEJ9DMt80wN?=
 =?us-ascii?Q?xLz+cDRSt6ZeO9EdAA3k9ZXLM5YHCAA6pIjMB27GWJKb0AOkVs7S565/qCvw?=
 =?us-ascii?Q?1egutgZtfYjdeU0IolCzdkhxXZWQDY3sVCAmccMiS4n+WVVpfwdBAtc+KNvy?=
 =?us-ascii?Q?+uOWrQeLkJtkxxY68xQL8nfr1ZolPDR+fibKwtnVn5eN6o1Z2/H5hwNSaIrK?=
```

```
 =?us-ascii?Q?BEIkcLggAervPWojykZ10NH5G1pfXb0nzNhIMyNI/m07NEZ6o24eUa2qBlOA?=
 =?us-ascii?Q?JWqXOYP2WAYC0kM4XztG5rxFERh7eXmgOAJNwjihmagGYUzQJtRs/3TJtgdU?=
 =?us-ascii?Q?UcnckhKEVevBe/u7I/a7y/LlYN/NB29sE8u/qRHB/gmK1WDpiuWiOrPdY4Cn?=
 =?us-ascii?Q?CVtZGl3pX3Eyi+S/4rVK+cX6t2YLPvkPVI/XNGHzIXruNXcAlI+/0Q8YGQNe?=
 =?us-ascii?Q?GfLYZfFe9dm26fP2T8CPIFhmS8Ckdl7fkkfg0svmVhVEJqovtSh1OunkrQI4?=
 =?us-ascii?Q?iF4AmyBNugErBY6d3QyhoU/i8MeJLwAzTU7DsbIJW6zsGkhHRwwP9V/W2bUh?=
 =?us-ascii?Q?Bi61kTSsXx43Yzta22upTKQSqvz1FtrmGlYtQyF/bwjWesFHo6zXXLuiGEMe?=
 =?us-ascii?Q?TSLPUjUS46C8l8XWxRFw3enyLIkm8s/gq8z1uU16HsjQGcSbgH6ZQSdwEsZh?=
 =?us-ascii?Q?/MR4aUWH8J1kLgUBri01A1nYePKSMc45Mg4gfWldqMRHM+KoUVK/E1PPIzLG?=
 =?us-ascii?Q?cKaFJ14jyIp9/7rokxKkCkK9+yQxdb4AGJNYkRNgAW+O45o2TW7hnKTNVyTx?=
 =?us-ascii?Q?5L0T2II2JjGS9KPDpvInroumjphtKVyZx9lGiMh9y32gq4HbfscFLY/zMuqa?=
 =?us-ascii?Q?6kNyHXgIkrYrOXcxqpKXKDUTRfsB23BZJflLqLWSWlLlhbV0vLoIR+CUl7nJ?=
 =?us-ascii?Q?IaONSBr+SnQXcmNxkDyCq7DmGGLisdx6bTmUU1j9rcgZPY00nF4my0JH1FRU?=
 =?us-ascii?Q?w6Pri8dLFfqfoWsKiCAEQbpTJvHv2h9wTpfV2c2Q/+UIkU8SC4l/VKdLv7Zk?=
 =?us-ascii?Q?APuVWk/FeVF2oIcGlcWCUIv7Qkl44L7F5VkNON4XMxPPUyGvcjqTl2sklhvC?=
 =?us-ascii?Q?GrFn4D83T1rXGVWWPWdqBJ34rdfQd0UbPL63wg=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: MN2PR09MB5515
X-OrganizationHeadersPreserved: MN2PR09MB5515.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT008.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(34756004)(26005)(1096003)(8936002)(6506007)(52536014)(82310400002)(83080400001)(10
9986005)(28085005)(33656002)(356005)(81166007)(7696005)(2940100002)(86362001)(833804000
01)(186003)(336012)(45080400002)(8676002)(7416002)(9686003)(166002)(450100002)(21480400
003)(55016002)(19627405001)(5660300002);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: b3501f52-03e7-4f41-f8bd-08d81cf6db63
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?biBnQqT5RkEMxAEqhD7Z4Dwh9elJ5Gmrq1WPWdqL6lZhgzqaWFkhbRWiUGar?=
 =?us-ascii?Q?Xjhf9io/Ao+HBS8WMNsBXyG4xSi5nNI14Jd4V2G9mz4mz6fw6kIFDOXjB1+B?=
 =?us-ascii?Q?BkZH19KATZaij4gf4RH7xhf73YGExxwHU7C1/Sap4oMAenLcb6gAGuNxGXEV?=
 =?us-ascii?Q?KXGmBB+h1U6V0rSbPOZvO5W3qgEnzJ/M0IgSJ+Ht29B2VMviSRmutqD1Whqb?=
 =?us-ascii?Q?S984njF8heEfVI0Ij5pjrHzcciO6ZN1XNgfhqQ0RQM/YuG9F1xJ/1pfbRCXT?=
 =?us-ascii?Q?QidEbXs08xf1daza4KnCLszucfXNP7Z/1MLjs8Wqqq6q7CpGvK8jyPxOF9zO?=
 =?us-ascii?Q?5fjDXF9JP/DhW1AJGV+QPYcwa3NZRcKdYypymFh+nHN4EbyaoLZJ1cuCu2yy?=
 =?us-ascii?Q?ouc59JgZGrfmbaxf2jRc0eTg55BRWaOo7+/AGx1RFvMr1gcdsOn7lsCo9SGE?=
 =?us-ascii?Q?AsPwVHGhNgrJwU0Uji6n0XtcnZerBW9G0t0P2szetYzYh8UcX3LU51HTK/MR?=
 =?us-ascii?Q?RlKULSse4Md4qZVwS4aksU6qc+T8lVXcoxUbO9Mj8pekNC+AMwDqFh8ZGC0Y?=
 =?us-ascii?Q?vBqeztyWirBubASKhOFmuX8N55208Yv/K+WB7A19f0rtGQbLPd3SGSCVcVEI?=
 =?us-ascii?Q?FWyePnbmIY2dTg5wqIty6kPdLWuJejASOpPmP5OYqUBQBI5u+Mcx9qAMmhHf?=
 =?us-ascii?Q?UhsM/uvnxsuMhgy9ZabSAnfwFLH9LmUy6aHL2IbH35kveZIInoKxyoMV604G?=
 =?us-ascii?Q?H8A7eZcaGDxRWkePHVfZWux8COGI1+ZC27wZWNjzV0nu1awHmRcp9t+CnfCY?=
 =?us-ascii?Q?EgaPYG3qvdO+zAtxFJW0A5hi3wgpjWtmwP/4nzjbPCjjVoo/BL7aWdyRTr7t?=
 =?us-ascii?Q?uwApHkiMVcyvf+wYcJOCHfUg3SFhdhFLmKxH+69fxyAcpx0ZqvznSBa+j+1X?=
 =?us-ascii?Q?lGYo4NhBeE9hLjRoUj69FNqrqWr9abOWXBDGjSwNqsubn0g/tFBAq6GTedv0?=
 =?us-ascii?Q?0Sa3Nr2evFFbRtvxZ+VPZ7qt+tPlCQ2HVkEMpyw3VfDpYiPfLQCSrIP/TKkY?=
 =?us-ascii?Q?4K8SP3KTOfMphyppyzg/lRd9QDOHV+bB8AJQqcdXEkaZzKgpIyc8p5PSxsd3?=
 =?us-ascii?Q?C5bj706fZuaGJ7Yu1tnKTz+0qcDVzxqgAUX77AQtxkg+l4TlvO3oIUPi5QxF?=
 =?us-ascii?Q?JkysUAa3jrXIfQ7oY7E25orEfGj5Xt6XUSO7wjobNJmrVjxWirLDmWSO9Ps3?=
 =?us-ascii?Q?7IPMiCen34stwmDbiXEQ?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: SA9PR09MB4638
X-OrganizationHeadersPreserved: SA9PR09MB4638.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT005.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(26005)(33656002)(450100002)(28085005)(34756004)(109986005)(7696005)(19627405001)(9
686003)(55016002)(45080400002)(5660300002)(8676002)(6506007)(166002)(7416002)(214804000
03)(52536014)(2940100002)(186003)(356005)(83080400001)(83380400001)(86362001)(8936002)(
1096003)(336012)(82310400002)(81166007);DIR:INB;SFP:;
```

X-MS-Office365-Filtering-Correlation-Id-Prvs: a58626f3-998b-4afa-b83d-08d81cf8f857
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?wpX/nsKEukMXOpuqLquwXjjTHKKptLX2VGOCK3yMIhAu/1IK176uFAru8mlR?=
 =?us-ascii?Q?9tRU6Xzha+zF+YVtaX5AbfIb9NABFLT8WDyB+Owz3t8usEN+h/yhYpDD8ysv?=
 =?us-ascii?Q?t6Xdz0kyKffsX9qMcKxYOkpIeIVqR95w72bfGCcbCULcKDPsXbAI068zLHrp?=
 =?us-ascii?Q?BWsM4AbNBXjSOIOan14rPfaN1MaOmZQxxt2DVVXJb2PorVg6AtbB4nsJJDda?=
 =?us-ascii?Q?OrusgELKg9w3/yCtLQCRHEz3GSBTl/7pNVRxXzpJBA6FkWGXDui8PlTM9BfM?=
 =?us-ascii?Q?eBKDiINw+xBnbNMKpIcN9g8aSCmr4htfI4i/lUlPZNE8bWseEhS90K7Gh7b2?=
 =?us-ascii?Q?By+yno5NFif1AQbEnP3+t3uqty3jNh/IkKkrBg2FxWkkTCkIIgCtyz/yuCt4?=
 =?us-ascii?Q?MP70pH3wIXy1NsbB0EUzgp2PP5RbdfqQvd25FlAk/fIh8BXt5bCwgd+Ax1/U?=
 =?us-ascii?Q?x+CjSJSTZPWjYVvQvyHt7Utk20d8T4ONiI0+hxXY45Wupyo63R1RLp9GVVY7?=
 =?us-ascii?Q?J8JS6onsSmYyslJGcbW0vfylYT+sXzsPHME+QiHqiGVBIc3ywSZGDirsikaE?=
 =?us-ascii?Q?mzBhYt1yxCcRAaZl0sgKOYPteEjefnUFV6FX+oz4Xh2tO1vq+fxrKYA9NXeC?=
 =?us-ascii?Q?1YcTes+X0Gz3VB9O/lUHm/gxSCJiKdjqEr/57bobFC+Zh7OE0sr3aBYllWLw?=
 =?us-ascii?Q?ff1mcdiPpZlTWs4KZA9NJ6jASCHVYO5sIJgj7GjFaZ6hMAwy7IX5CDZOJISb?=
 =?us-ascii?Q?TyQrc5CFC30dsfvXRN/Jv8fKE4bUHyi6z46MObCbGdoj8d+Nnyk7V02qWNH7?=
 =?us-ascii?Q?1zpAXHTl9sHMJ1bBn7DcH0s5fhjSpYqN0bIP4dG/TlY2+V1oXp/0b0sqeVnR?=
 =?us-ascii?Q?k3oIRMyf9h4vgZddELfiiOyZgW91st0tXPqyerdG1G6OLdPFxQc+Vv3S9bd4?=
 =?us-ascii?Q?fPqoLvVMYdfPVMDc3+bl87MSjIZgOdJqRzckjphxsMFLLDPrutep4pEcXcOp?=
 =?us-ascii?Q?jnwfJW1xZ1lDEi/1+MOEwe1wU67SZj1Ux0rsou2SdoAA1ftgVrhju2MuPL+x?=
 =?us-ascii?Q?hpcOm1Ewv87ajT9WAlgpOq2SP9NM0bZLe0HHyWoO0276vZQLsDWb6du/WMhP?=
 =?us-ascii?Q?7qFcSxwUkAfkMc5INYtxSFV1BZHTBb60SNrw2PCbBQOw5lR1qIQ8yxfIS1+a?=
 =?us-ascii?Q?vrk52/FHpERb3/eW59/zRpdWMCwYVI2z+Vz5+w=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: CH2PR09MB4588
X-OrganizationHeadersPreserved: CH2PR09MB4588.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: CY1GCC01FT010.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(8936002)(1096003)(2940100002)(86362001)(186003)(26005)(34756004)(28085005)(1962740
5001)(6506007)(5660300002)(21480400003)(83380400001)(336012)(8676002)(450100002)(741600
2)(45080400002)(82310400002)(109986005)(52536014)(55016002)(33656002)(9686003)(81166007
)(7696005)(83080400001)(166002);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 6f58c0ff-fc9f-4f7f-2bd4-08d81cfb172e
X-Microsoft-Antispam: BCL:0;
X-Microsoft-Antispam-Message-Info: =?Windows-
1252?Q?JAU9k41FY5x9/Fy+KKg8XjO2wL3CvH2UyAQ+veIk8xb7Ey3xTXDxiDtI?=
 =?Windows-1252?Q?M4UwLXU8/tPhV3Oq5aYmyElNumSW5VjGMVUAq/PXopVwCTiFMfHGJnMW?=
 =?Windows-1252?Q?Gq8Xt2c7TcLl6HIMDOslMgdTr75xaGYBww7UrheHhV7EnIUz3ImwDq4J?=
 =?Windows-1252?Q?kyt/a3y0Mvp573uwnaVIiCrMUJVEuIbU+p6v455e3sEjIdkZrIafFXCO?=
 =?Windows-1252?Q?XXmqLxIRjhZtEbsdbWrg1462bvX64p7Q2EHFBVHd0HckJzQP/CT2jAJ5?=
 =?Windows-1252?Q?3wM8/H9+VRXwu7W2lVaKKmiXGHydUP4L1x1m1+9Kooq8FzrZ3+vKg/BU?=
 =?Windows-1252?Q?kK/OUiuF1L4dCQDmBEjlXkvDB1t/d5LJctIqvi0lLSJlLTRw7tmxAcvb?=
 =?Windows-1252?Q?9xA6tYw7lOKKRTaPH+UbGGLNHY5uZ7ACndzve9IZHCyftlyNe1dkP2O7?=
 =?Windows-1252?Q?1Q6tBHBf8IAAJcHfSde6eJVNj8fs+cJkL5v31AjCYvlqMObh5M8vnWVU?=
 =?Windows-1252?Q?9R/RELmO+gblSLwq4UDYnwF7krT5iM9l4xh9k6yXe6/rFV0DODnfNnPP?=
 =?Windows-1252?Q?JmBlMJUgu4jPXs6aFZHEily9FUnmFcEbOn2vSLoOiRrovr4ip3meB92a?=
 =?Windows-1252?Q?ZRmF/qBewNbl0bf0kYJOZ1ngAUMDKrOBZ7Hm099L1xyDuren7zu2ZefD?=
 =?Windows-1252?Q?dALOavGamCnil6U5mNc0XrrvgBcPotCYGsbDHm7TAlvz4YgWBIsjeHHA?=
 =?Windows-1252?Q?XpxgAbyJQigCMrK6ddboeA8Is+2gz6j7f7yBllXApb6NjiQY70rwqiFf?=
 =?Windows-1252?Q?YdNY8LYUi2lXUAl455S+/7BEEdTLuPYS0bCm3qwvOp3Ak5nr2ExRaQaj?=
 =?Windows-1252?Q?K11VwdJIjtraUjzngzYQ6JkpGd7QLs7okDb33R5q/WVGao5dj5x5Nhy3?=
 =?Windows-1252?Q?0q75qsZfd9G6UoT6BKReciMCvMqmeysgxFaWysEdaYQSBTDvpqdwLlq+?=
 =?Windows-1252?Q?N623W8ESOAbGQRRivJvVLxDVtTEhzWGR+o2tg86ITZJd9lMaF+NxxPw/?=
 =?Windows-1252?Q?TF9E4m/KOJmlV285G5PHqi/q0ez8Ax5I8ta6UXwBVyU8v2lsG73WnemO?=
 =?Windows-1252?Q?/S3LVEHOk4LIvRdlMv9JAeIryzzKFhOYo0rqaKQnRUjqpa50LMaEUH9M?=
 =?Windows-1252?Q?23iSn6jpk/C7JSVJ+2CU/XzsfShFwgHjKcFEjUoImPFSk/3mitA1edEs?=
 =?Windows-1252?Q?5LN4tLt/wX4eSnx+mdhC1rWmcDI4zIDFxdFah8PVHfifeEKmVFPk4puo?=
 =?Windows-1252?Q?XSJgo3vrMRySesdgHOM3CLWYMUPvcdvFaXt0NQLTkhLmlp1x?=
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 30 Jun 2020 13:40:37.7362
 (UTC)
X-MS-Exchange-CrossTenant-Network-Message-Id: 4e80628d-db46-4c13-8d96-08d81cfb2c49
X-MS-Exchange-CrossTenant-Id: 8b4d55ae-6db4-4e05-a85c-59d6a256cd6e

X-MS-Exchange-CrossTenant-OriginalAttributedTenantConnectingIp: TenantId=8b4d55ae-6db4-4e05-a85c-59d6a256cd6e;Ip=[162.217.184.79];Helo=[CCCASV01.CCOUNTY.com]
X-MS-Exchange-CrossTenant-AuthSource: CY1GCC01FT010.eop-gcc01.prod.protection.outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Anonymous
X-MS-Exchange-CrossTenant-FromEntityHeader: HybridOnPrem
X-MS-Exchange-Transport-CrossTenantHeadersStamped: MN2PR09MB4843
X-OrganizationHeadersPreserved: MN2PR09MB4843.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredByDsnGenerator: CCCASV02.CCOUNTY.com

Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	CCSO Intel (Sheriff) <CCSO.INTEL@cookcountyil.gov>
Sent:	June 30, 2020 8:07:45 AM CDT
Received:	June 30, 2020 8:40:40 AM CDT
Attachments:	(U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

Please see the attached DHS Intelligence Brief, “Criminal Hackers Target US Law Enforcement Data,” dated June 29, 2020. A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

If you no longer wish to be on this distribution list, please send an email to ccso.intel@cookcountyil.gov to discontinue receiving these emails. If you would like any member under your command to receive these emails, please send an email to ccso.intel@cookcountyil.gov and include their name, title and email address in the body of the request.

Cook County Sheriff's Office
Strategic Operations Center
3026 S. California Avenue
Building 5, 2nd Floor
Chicago, IL. 60608
Office: 773-674-2694 or 8477
Fax: 773-674-4797

THIS IS A CONFIDENTIAL LAW ENFORCEMENT COMMUNICATION. The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential. If you are not the intended recipient of this message, or if this message has been addressed to you in error, please immediately alert the sender by reply e-mail and then delete this message and its attachments. Do not deliver, distribute, transmit or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action relative to the information contained in this communication and/or attachments. This e-mail and any attached documents may contain For Official Use Only and/or Law Enforcement Sensitive material and should not be disseminated outside of official law enforcement channels. The information contained in this message as well as any attachments shall not be released to the media or the general public.

Undeliverable: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

From:	Microsoft Outlook <MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@cookcountyil.gov>
To:	CCSO.INTEL@cookcountyil.gov, Eric.Sellers@cookcountyil.gov
Sent:	June 30, 2020 8:56:06 AM CDT
Received:	June 30, 2020 8:56:10 AM CDT
Attachments:	Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

Delivery has failed to these recipients or groups:

Eric.Sellers@cookcountyil.gov
A problem occurred during the delivery of your message likely due to a bad mail routing configuration or mailbox rule setting. If the problem continues, contact your email admin.

The following organization rejected your message: CY1GCC01FT003.mail.protection.outlook.com.

Diagnostic information for administrators:

Generating server: CCCASV01.CCOUNTY.com

Eric.Sellers@cookcountyil.gov
CY1GCC01FT003.mail.protection.outlook.com
Remote Server returned '554 5.4.14 Hop count exceeded - possible mail loop ATTR1 [CY1GCC01FT003.eop-gcc01.prod.protection.outlook.com]'

Original message headers:

```
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
 (10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
 2020 08:40:41 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
 by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:40:41 -0500
Received: from DM6PR09CA0026.namprd09.prod.outlook.com (2603:10b6:5:160::39)
 by BYAPR09MB3189.namprd09.prod.outlook.com (2603:10b6:a03:a5::23) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.24; Tue, 30 Jun
 2020 13:40:39 +0000
Received: from CY1GCC01FT010.eop-gcc01.prod.protection.outlook.com
 (2a01:111:f400:7d02::208) by DM6PR09CA0026.outlook.office365.com
 (2603:10b6:5:160::39) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend
 Transport; Tue, 30 Jun 2020 13:40:39 +0000
Authentication-Results: spf=softfail (sender IP is 162.217.184.79)
 smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
 header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
```

cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
CY1GCC01FT010.mail.protection.outlook.com (10.97.0.149) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:40:38 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:25:34 -0500
Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:25:34 -0500
Received: from MWHPR09CA0028.namprd09.prod.outlook.com (2603:10b6:300:6d::14)
by BY5PR09MB3873.namprd09.prod.outlook.com (2603:10b6:a03:1fc::19) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20; Tue, 30 Jun
2020 13:25:32 +0000
Received: from DM2GCC01FT007.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::200) by MWHPR09CA0028.outlook.office365.com
(2603:10b6:300:6d::14) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
Transport; Tue, 30 Jun 2020 13:25:32 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT007.mail.protection.outlook.com (10.97.3.159) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:25:31 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:24:59 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:24:59 -0500
Received: from BN6PR09CA0054.namprd09.prod.outlook.com (2603:10b6:404:7a::16)
by SA9PR09MB5439.namprd09.prod.outlook.com (2603:10b6:806:47::13) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
2020 13:24:56 +0000
Received: from DM2GCC01FT008.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::206) by BN6PR09CA0054.outlook.office365.com
(2603:10b6:404:7a::16) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20 via Frontend
Transport; Tue, 30 Jun 2020 13:24:56 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT008.mail.protection.outlook.com (10.97.3.193) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:24:55 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
(10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:09:48 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server

(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:09:48 -0500
Received: from CY4PR09CA0074.namprd09.prod.outlook.com (2603:10b6:903:c7::12)
by MW2PR0901MB3819.namprd09.prod.outlook.com (2603:10b6:302:6::17) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.24; Tue, 30 Jun
2020 13:09:37 +0000
Received: from DM2GCC01FT007.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::201) by CY4PR09CA0074.outlook.office365.com
(2603:10b6:903:c7::12) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
Transport; Tue, 30 Jun 2020 13:09:37 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT007.mail.protection.outlook.com (10.97.3.159) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:09:37 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:08:30 -0500
Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:30 -0500
Received: from BL2PR09CA0006.namprd09.prod.outlook.com
(2a01:111:e400:c743::16) by BY5PR09MB4181.namprd09.prod.outlook.com
(2603:10b6:a03:1d8::9) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20; Tue, 30 Jun
2020 13:08:28 +0000
Received: from DM2GCC01FT005.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::206) by BL2PR09CA0006.outlook.office365.com
(2a01:111:e400:c743::16) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20 via Frontend
Transport; Tue, 30 Jun 2020 13:08:28 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT005.mail.protection.outlook.com (10.97.3.0) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:28 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:08:19 -0500
Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:19 -0500
Received: from BL0PR0901CA0022.namprd09.prod.outlook.com
(2603:10b6:208:1c0::32) by DM6PR09MB5639.namprd09.prod.outlook.com
(2603:10b6:5:261::18) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20; Tue, 30 Jun
2020 13:08:17 +0000
Received: from DM2GCC01FT006.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::203) by BL0PR0901CA0022.outlook.office365.com
(2603:10b6:208:1c0::32) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21 via Frontend

Transport; Tue, 30 Jun 2020 13:08:17 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT006.mail.protection.outlook.com (10.97.3.107) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:17 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
(10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:08:14 -0500
Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:08:14 -0500
Received: from BN3PR09CA0048.namprd09.prod.outlook.com (2603:10b6:400:3::16)
by SA9PR09MB5678.namprd09.prod.outlook.com (2603:10b6:806:1d::23) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
2020 13:08:12 +0000
Received: from DM2GCC01FT009.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::207) by BN3PR09CA0048.outlook.office365.com
(2603:10b6:400:3::16) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.20 via Frontend
Transport; Tue, 30 Jun 2020 13:08:12 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV02.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT009.mail.protection.outlook.com (10.97.2.68) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:08:12 +0000
Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV02.CCOUNTY.com
(10.124.40.40) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
2020 08:07:55 -0500
Received: from GCC02-DM3-obe.outbound.protection.outlook.com (10.124.186.250)
by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:07:55 -0500
Received: from BL0PR0901CA0008.namprd09.prod.outlook.com
(2603:10b6:208:1c0::18) by BY5PR09MB4136.namprd09.prod.outlook.com
(2603:10b6:a03:1dc::9) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.23; Tue, 30 Jun
2020 13:07:50 +0000
Received: from DM2GCC01FT006.eop-gcc01.prod.protection.outlook.com
(2a01:111:f400:7d01::208) by BL0PR0901CA0008.outlook.office365.com
(2603:10b6:208:1c0::18) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3153.20 via Frontend
Transport; Tue, 30 Jun 2020 13:07:50 +0000
Authentication-Results-Original: spf=softfail (sender IP is 162.217.184.79)
smtp.mailfrom=cookcountyil.gov; cookcountyil.gov; dkim=none (message not
signed) header.d=none;cookcountyil.gov; dmarc=fail action=none
header.from=cookcountyil.gov;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cookcountyil.gov discourages use of 162.217.184.79 as permitted sender)
Received: from CCCASV01.CCOUNTY.com (162.217.184.79) by
DM2GCC01FT006.mail.protection.outlook.com (10.97.3.107) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
15.20.3131.20 via Frontend Transport; Tue, 30 Jun 2020 13:07:50 +0000

Received: from CCCASV02.CCOUNTY.com (10.124.40.40) by CCCASV01.CCOUNTY.com
 (10.124.40.39) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1261.35; Tue, 30 Jun
 2020 08:07:25 -0500
Received: from GCC02-BL0-obe.outbound.protection.outlook.com (10.124.186.250)
 by CCCASV02.CCOUNTY.com (10.124.40.40) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id
 15.1.1261.35 via Frontend Transport; Tue, 30 Jun 2020 08:07:25 -0500
Received: from CH2PR09MB4491.namprd09.prod.outlook.com (2603:10b6:610:36::19)
 by CH2PR09MB4395.namprd09.prod.outlook.com (2603:10b6:610:6d::18) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3131.21; Tue, 30 Jun
 2020 13:07:22 +0000
Received: from CH2PR09MB4491.namprd09.prod.outlook.com
 ([fe80::54b4:1a30:151b:810f]) by CH2PR09MB4491.namprd09.prod.outlook.com
 ([fe80::54b4:1a30:151b:810f%5]) with mapi id 15.20.3131.027; Tue, 30 Jun 2020
 13:07:22 +0000
From: "CCSO Intel (Sheriff)" <CCSO.INTEL@cookcountyil.gov>
Subject: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement
 Data
Thread-Topic: Pass Through - (U//FOUO) Criminal Hackers Target US Law
 Enforcement Data
Thread-Index: AdZOUZRVrVUDcfOlTiiWh3YE0iFXiAAjZyaaAAAHqe8=
Date: Tue, 30 Jun 2020 13:07:20 +0000
Message-ID:
<CH2PR09MB4491104495F32B729B402EA7F56F0@CH2PR09MB4491.namprd09.prod.outlook.com>
References: <LYRIS-103909956-1411846-2020.06.29-15.13.38--isp-les-
north#lists.illinois.gov@lists.illinois.gov>,<CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH
2PR09MB4491.namprd09.prod.outlook.com>
In-Reply-To:
<CH2PR09MB44918DBCA1539E418B6FB17FF56F0@CH2PR09MB4491.namprd09.prod.outlook.com>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Authentication-Results-Original: cookcountyil.gov; dkim=none (message not
 signed) header.d=none;cookcountyil.gov; dmarc=none action=none
 header.from=cookcountyil.gov;
x-originating-ip: [162.217.184.194]
x-ms-publictraffictype: Email
X-MS-Office365-Filtering-HT: Tenant
X-MS-Office365-Filtering-Correlation-Id: ae69832f-1896-462e-8066-08d81cfb2cf6
x-ms-traffictypediagnostic:
CH2PR09MB4395:|BY5PR09MB4136:|SA9PR09MB5678:|DM6PR09MB5639:|BY5PR09MB4181:|MW2PR0901MB3
819:|SA9PR09MB5439:|BY5PR09MB3873:|BYAPR09MB3189:
x-ms-oob-tlc-oobclassifiers:
OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;OLM:9508;
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original:
i+uzE6hVIcnRsGS1QWcn6TsXKHhKrGB2ApYs8WShxLg2UpOu82OHRfhsFp+9CjlQecvSzZCwXpa1AWO4qrntWsl
2q6Qw2oMnjCqqm1vLhbB607gMDIp2f7mBL3QYwDQr+r4wNnGRAC9xe3+5GPOy8gs0xnYC/tzY345eFTIOdpxi8h
rvmE/ovgAyrKD2M+aVOHraAlD6Yg0/dp+AIa6uQJHM92dDHc+v9NmfffieN4nF9HU5Sho5QfaoyzaceI9B/Iqgk
rVdjSZovu2pQFCekwDl0jsQ53n+eomH8b9QGuQEKneL2evjWMOddw0zd2moDdY/WDuTaKA+WaJWmCPW1pOPTjZL
1592rts6hC49p2A=
X-Forefront-Antispam-Report-Untrusted: CIP:255.255.255.255;CTRY:;LANG:en;SCL:-
1;SRV:;IPV:NLI;SFV:SKI;H:CH2PR09MB4491.namprd09.prod.outlook.com;PTR:;CAT:NONE;SFTY:;SF
S:;DIR:INB;SFP:;
x-ms-exchange-antispam-messagedata:
BuYbw0RoSBfECmAFs5sfpqFR/eESsNr+Plx06kdsYiyNoXFEYgS3Jz6QYqBwqda1BgTm5iebI1sncXRB6v4+RaV
C42PElOHwFJBOAzNHKMxkCZCwRx1mubguafevanh98UlGYiSoqtiVFIMyzzqWjVwq2ALgG6TEoWTOD6wL3DH1g+
twaRUDU5pX7Y3UuqHnjSUkkWpE3g+KMrlKiWDb6hsqAZsExSu0dRsfe1bY5iawMgV1P06KM54AE4iNVyJ6s+PhZ
oFB021MJN0zbzrKRmG5l76nAVkDQZ6LAJ59qRaYnm4V2jeg+UrmezaEA1BSTXRnJE7c4PTWoAZR7vsnGJlZPDSr
wlqBu5V9fQ0asbFFrSOauG9RYEIceEBMj2qfNX9W5sCwVf+Z2W+dW0tMy5YgF7ghw6XrerqzMMShABB14TwG3sg
hMkbytZTnSmqwnqf05E2cPgyZHNVzIQHTfXbIbLbhC/u0Vat8cAb+p0h0NzcOhHtduUMJV/CgNncT
x-ms-exchange-transport-forked: True
x-ms-exchange-transport-crosstenantheadersstamped: CH2PR09MB4395
x-organizationheaderspreserved: CH2PR09MB4395.namprd09.prod.outlook.com

```
x-crosspremisesheadersfiltered: CCCASV02.CCOUNTY.com
Content-Type: multipart/mixed;
      boundary="_004_CH2PR09MB4491104495F32B729B402EA7F56F0CH2PR09MB4491namp_"
MIME-Version: 1.0
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
To: Undisclosed recipients:;
Return-Path: CCSO.INTEL@cookcountyil.gov
X-EOPAttributedMessage: 7
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT006.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(356005)(8676002)(33656002)(34756004)(9686003)(45080400002)(186003)(19627405001)(83
080400001)(28085005)(26005)(81166007)(86362001)(7696005)(2940100002)(6506007)(833804000
01)(21480400003)(55016002)(109986005)(52536014)(8936002)(1096003)(166002)(82310400002)(
336012)(5660300002);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 03205142-5935-4a88-f6ba-08d81cf68713
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?1YLt41zjohYS1UQWgvO6t91rCCqmdNXNGL/1ZqlPhd8tDb34+hVkCmKjQgwb?=
 =?us-ascii?Q?lE0v2qaDx+WsLhCBH/P6FoIGXDyGtPXI+a59WXVg18wHNZnTDW4ezihvX/C/?=
 =?us-ascii?Q?C5QWIwG1jMZ9nNide/BsVAQCvRtiOiBwMJzJgBHWppSXiCqkYXvAjVrFnthB?=
 =?us-ascii?Q?/lELoNNBfU9gEfGdSrA4hMYtLJGDZPcIMU3mertlD3yhJUsvE76hl7dLvwhp?=
 =?us-ascii?Q?obmlOpUj8JfbMLumE4IOLNi3SRsSiKMXRl84tmPxF0ZLtLLQAb5L9QyUIRGj?=
 =?us-ascii?Q?AfagIBxOE8rFB7FQ7Tmiso+NUhQlVuQ2CsnbG0tQXYw6kOW7j4L2SpghokBq?=
 =?us-ascii?Q?snBb4X+vH3byJAS3RBbnw8FUqDwI9bETbypLZW/ATea7NHqtwh2NL9ulpmGR?=
 =?us-ascii?Q?SOKVOBDBl06C8xcScJqRr6TMd6f/QSG9RS/o5mY8sLeW4QUgPRdc+l9G9U8i?=
 =?us-ascii?Q?xgh0C1lmeXsOOPAvFGOqUuHuq98fuK/h3dJe4ol9ldndrl25/ZrD5/mM5tMU?=
 =?us-ascii?Q?Cika3DJc6ThxpEhVk9eP0XF3vXsSyLh/5lVqggK7qdIo9Or4L+EytEBmagiP?=
 =?us-ascii?Q?90IvfBUZOTqvL+YXRh5IthlNKY2KnaVm4ZEIZZIsappdmR1fbX+8jwfaClt5?=
 =?us-ascii?Q?Mvy6KqTV7nvG67X+4sZJ1UYJUlOpWnelosGHA2cKePDx2irAzAo8+CfMuHMd?=
 =?us-ascii?Q?VLPTAEvFysFosJbqc8KyJ9bAGPILhmxmPOtJSxglO8YO94MHpb8WFSt8YcOH?=
 =?us-ascii?Q?J4j9Puchb642Tgo7/H5YBoydy6KVYd0HtiqpM/w20pXyLDjFIcPYC+AxAobp?=
 =?us-ascii?Q?bNbiYMYfeW6InJRy6J5FW9UOBuhpSD8hW5nL4XrqLTXT1ANdkZuSZGM/ia8s?=
 =?us-ascii?Q?dFg+kVtAn6Dw/aJj0DLtjFC+ddjmWFkqsJvSRiQhUVNR9IJKn7T984YX0LM3?=
 =?us-ascii?Q?Hv+6+vtPrSi+DCE5A3wynhr+LiTnpObCZ48EEHmqqth6RqHH094c+Kvyy98E?=
 =?us-ascii?Q?I3n3ipWylznaSwyRpDpXq5G1tc2ItHjwxa/sKDfZ4Z5XaQjJPpgv5GdDq1yr?=
 =?us-ascii?Q?kkb0rVr63pPAcpNLufGDhekFCMrU12CenZmbYwKHR0jdtlCWZGjP47fvj8pU?=
 =?us-ascii?Q?u9H4IvIJEsgVHua/lah2OG865xn68nQdfx+rdK1A34m+O0nnmZT7I6nrGWhp?=
 =?us-ascii?Q?2cCqDlyKKbI9vRaAmGMYDULh937oq9QdOJZptg=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: BY5PR09MB4136
X-OrganizationHeadersPreserved: BY5PR09MB4136.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT009.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(5660300002)(83380400001)(6506007)(45080400002)(186003)(9686003)(55016002)(336012)(
7696005)(34756004)(28085005)(26005)(109986005)(8676002)(166002)(2940100002)(21480400003
)(52536014)(81166007)(86362001)(82310400002)(83080400001)(19627405001)(1096003)(8936002
)(33656002);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 87167387-01ce-46e6-dbb8-08d81cf6977c
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?8OirdlrP+4M9ZUrarYwhqR8i7U86kRgTKTpoySUWUyssajlzkCeqYYNOuYU+?=
 =?us-ascii?Q?3QuYqtfaRv1soOEriADWywpccebe3ILn7BRHmi69S8svxONn3HC5/nV1fhJ3?=
 =?us-ascii?Q?Y7bDDoU9jA0Xvd7tG9tRM1TNiZtcs5kbYdc+TduZXYeFbGUZhAAMO2ovvHin?=
 =?us-ascii?Q?4lKF1qrIjmco91z55JWEc+JYv5FQ7HyqpDym4N8GbuJ3m969QQxizQ+Ru/V0?=
 =?us-ascii?Q?3YQGzNpg9ACRBgCTjxd+2xQqDD+W7aW8WyO6SV4Tpqt1T4Qt6ovBv1qE+gad?=
 =?us-ascii?Q?apnoIIF4CAMFKDakZlRXBUC4UjK4fH6nAy7Z1GLBDah1OL/av+lFxGyBUYvx?=
 =?us-ascii?Q?jZprMhtwvHmg/3VuLiuze0Q/qk1HNFtUX7m7aQjVhJodpD7PjPkGTWveDbmF?=
 =?us-ascii?Q?Ayx63s05wC0VYQYiQCXfRaBtmJMCQezNOZ0IvLEgJyk3m7zKZTOlnmkdjSZV?=
 =?us-ascii?Q?MjDgs9HClINF3xd0cgll5EzOc2vAEP39yXSuDznLNW6DNXkM2moPtqhN3zfR?=
 =?us-ascii?Q?t+R8TTMR+kc/kt5T+qi3YMMolCHUEqZagUZged48yWjp3IFRBTduhmv5vyU9?=
```

```
 =?us-ascii?Q?R/QVoaoq1LuVUWpakQTA9mmYlbR409tUofmD6b6/q7DVTRC84QPpytyLfigX?=
 =?us-ascii?Q?ZE8cR5mDpE0Ho1D0gwFkBX+OUwt2c2+QlFFCr35uo+eQuGXdfG/r0G6IBRzJ?=
 =?us-ascii?Q?0ix07aUA/dhmckDxZxdVMfLwa3uLpYXwHTo4fDh3lJTxZhEv7SwzmIsgrlC6?=
 =?us-ascii?Q?/GLOKIiynnX4Q5uh514GfKuy3cUXJbS3ymWRhYAhgoIMNh31ZyKBKnMFzpOD?=
 =?us-ascii?Q?XLeY4kGvXf7gYULJ0gCwoGZtl5FanF2f6BRNtvQqifPIQu3JphDOGE/3Zqm4?=
 =?us-ascii?Q?uv3EZsuVjHDjPd0Db3WIoyHcZkLxFMFsua6oTOQwpsr0NK0XFQcovh2z8Lyw?=
 =?us-ascii?Q?P/4BIPW6bHiERotTLr5WWzhI9aLsPlSwir3esH6lMLCpY0eXKZldwdKwoHc+?=
 =?us-ascii?Q?uU97YqHOweP/CdV2EJtrdJJKJ6SYpGpcz+R6g3zIvCVGnekdsfQLZfjPGx9v?=
 =?us-ascii?Q?bT1h7a/zI0EeMJmTFKpCTo3d5zSZJHXhldAqFR6xEKI3WqqP+V4pS2o5VuP0?=
 =?us-ascii?Q?AzmQZUZWRL7hkQf5Vwl738DqhxUNHVb1n8AnM4rpRZ9A1xX8IVtTXlFuwuyX?=
 =?us-ascii?Q?CeH0yAzlm95KOoSwEx2a6+epAPGCZT+oKHodRg=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: SA9PR09MB5678
X-OrganizationHeadersPreserved: SA9PR09MB5678.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT006.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(33656002)(21480400003)(52536014)(2940100002)(86362001)(5660300002)(83380400001)(33
6012)(26005)(83080400001)(166002)(6506007)(34756004)(28085005)(1096003)(8936002)(867600
2)(82310400002)(7696005)(186003)(45080400002)(81166007)(356005)(9686003)(55016002)(1962
7405001)(109986005);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 1af24fbe-ca47-444d-331d-08d81cf6a495
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?d9dMEt6+zcNTF+V4eNF/sxeIvQRbdt/OGl60xLwXKaX6IQfo9ruQQdVNjSmH?=
 =?us-ascii?Q?iAl4GyTox43ecgePx8jo89W+wByJ8jqXMWC47nQ0rY6TdIlP2MBv5fyPwBcz?=
 =?us-ascii?Q?xAc4qv1UyVrthQnBW1CYer6oZRYuPQbwrRvkBL1eWOPBjJ4UtkBQfJo+rOvr?=
 =?us-ascii?Q?qnsBP3hauSorAZKN+YqZXYgileKP/YuhxUQicikiL/11W4aVhPKZQ7Lr5RZ9?=
 =?us-ascii?Q?v/jPE11CsU87POaEJw8HRmOqM+QpxayOSMPCpM5+lxnRV1zs3CGJwr+JB9Br?=
 =?us-ascii?Q?QSgttEN/TLq/aZ8LOuXTPFpvBGgLERFtRHWu/CjtKUb8BW7u6aWdYUNmJyYl?=
 =?us-ascii?Q?uOsyhVPFcgNP238j70QtIErZ+HNNiy8ATjZmqEAKdTD3A8ZNi1X6OLT8I44G?=
 =?us-ascii?Q?fJIOi5s+R42n8hHTkHx7uIciIWt0hixKVqvij7h8Y+ozQA4Pr+E3QYZtIzEK?=
 =?us-ascii?Q?/AKPJJQIGzrN0ue4gcDNEDIoeug5AEvaW+lbzj8lZR4hPVpgyA7xdYfpiyFh?=
 =?us-ascii?Q?PmIab8hznaH8m+bm3+hXFDbpfVrz3+lt8sRt77QNyDr28WUjlcQ65q/ayc5A?=
 =?us-ascii?Q?XSqMNyNINc4gGTjgjz2TsJgrtBEzY8mwb7+06Zvt0byqHSKXJ1H0OQjgjfxk?=
 =?us-ascii?Q?VX56BxMANMc7oysbOlECuUmGHLavNa3jn9k1+HsgE8aF9Cza5qsu8BgubBNy?=
 =?us-ascii?Q?ywj/c/cxp6Tg8TwRbD2qC3na5kSMETJnnEoFcOVkxSpYcb8wz5eRH7IvpLkt?=
 =?us-ascii?Q?DBhgbfZfIghEthUnTpqmhot4b5qTE2kSKxd2idFGbdyOfHV4kN4U3VPB6Obh?=
 =?us-ascii?Q?qc30ZiTXWbBtP0Fbp98K/QrN69YDoz4T8J06gnVFw6dPOMpQkZyECB+wzZ0h?=
 =?us-ascii?Q?YDLUn6EFGzDnsMglaB7F/xWmYWoo8CVjAnHgGBWR3mHWKyymX4FvTPjmiyK8?=
 =?us-ascii?Q?6igMckgb63ERixgZ9Woxp7JX3wnQc4ygqzpFOWdhlJCyt9R/UB/oaMI6tgrl?=
 =?us-ascii?Q?/+SiCU28VPq/X3+Kbf++MQ49EFL4R9nZXgN3gXNAf1/hGCy6WN3GxCz05soB?=
 =?us-ascii?Q?iHtDQVqxhdh2N3uHBNWIQbAfv8niSLUMjhj1vC/18Y3CT4wvXRuSNQVQIPhs?=
 =?us-ascii?Q?dWuOAdnOwcskT2khrdJwrv4jdkng7qFx17X1zQGx96o11VZOcQyQxndcaX7i?=
 =?us-ascii?Q?tm8HXuU3v3to8TA6P/iKFfKu9E1sO9AjqyOFYQ=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: DM6PR09MB5639
X-OrganizationHeadersPreserved: DM6PR09MB5639.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT005.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(19627405001)(336012)(109986005)(7696005)(34756004)(52536014)(8676002)(83380400001)
(28085005)(86362001)(186003)(6506007)(8936002)(1096003)(33656002)(45080400002)(21480400
003)(55016002)(9686003)(26005)(166002)(356005)(5660300002)(2940100002)(81166007)(823104
00002)(83080400001);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: f8e8296f-9d4d-4f39-aee8-08d81cf6a7d0
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?RkGcQjZPrbQ1Xo1BD1YvtuGzhkuLTuNhZQIFzlseHTbdDpv/5Fad6wBkKYKE?=
 =?us-ascii?Q?eNu0l4KgjHJE+uj+RrgQxnf4q0bSH28eqWZhxhla7m3O7/8HfpHfjzn5DtPy?=
 =?us-ascii?Q?meKzBUZjY2QZ+nP1+BfGIsZFDAv0Fi5KvMK5uT2CLcbKHk+jo4/3NH80vHla?=
```

```
 =?us-ascii?Q?aS7VKnUuMYx18UuA4qI/OS+/kYhCOOLtDMtKXdPtelfQ/vdqqv9O1ljox3yR?=
 =?us-ascii?Q?x3oHzYiugiBV5373E+iXpfdZbqUIkcQioI9/F351/3/j/J815mwHCM8o4Re9?=
 =?us-ascii?Q?zSixr8JSSytBVn8+WFfWovh9kpyQDVq561P97I2h11uQXljQfk1nfeRIjuM6?=
 =?us-ascii?Q?eohhgKKLRmTZUyB7MiYIsaZJ98P0yntbISW938tf5uah0yag6wnRUr4UTO7O?=
 =?us-ascii?Q?0FxX8U/Z08p0xG1I4mNPTT6xj030kcSUDPSU86dynJtbsvzbbTMqxPRLS+2W?=
 =?us-ascii?Q?yxHS9pBfwsFeehFexZWxfPcVOGBNKxqObMm5eZvCCj3m6kYC+fYG/l1fsW1O?=
 =?us-ascii?Q?wuzEfQzLF/6r2W/oXMzkASjNY1SpZSz3/1k3uwUVoJllPtMfAhORjDw1RTSm?=
 =?us-ascii?Q?DiSzWpz/lO2ZCT4ur42Vj9keSWmtK1TDKZYFldIxJ3f1fT/q1w8eC+yeaWYq?=
 =?us-ascii?Q?DDffbUMuUkTH/NeUTJvWIifJ8nhdZAs6yjqxm7s4cBN5wATkT3LC9HOFsp41?=
 =?us-ascii?Q?bRsPcdqG6cfKwJNTAo++1dPYffdTTlgmRPq3Xf9YkqBQF+3KjQ+VFOVi5K60?=
 =?us-ascii?Q?RAwhDPpZww2yY9ryKetsgunh9q0SUjieomU/3/0Vr153pmIEFE/E+90PwjDs?=
 =?us-ascii?Q?dEj5R+DvNfM3Ne548dJor8/CIXGZy3vGUiQqLylB/B3BJFX7HCHROxEZZrev?=
 =?us-ascii?Q?F/6TbqAFzM1ytbNtOxDphpjZgT6hbSbLDqqJppfLyyRT5KBmS3geYRLVx773?=
 =?us-ascii?Q?xnGKwHuoV854HK0ZiRw7rnAIy7Q8sxWnPnIc1oxeJ6T7dAFC0u/86CeIP4Yl?=
 =?us-ascii?Q?llfsfyPlCyVVKgdRIpem4bVGzve8f+DzASVYsyo3fYL9V8Xzhl9x97TInWeT?=
 =?us-ascii?Q?deIfzylz7vYMczFDDjZPI4Q/UNOVGGEsED0kmX5g11y2Db3TB/Ec9oEjfXa6?=
 =?us-ascii?Q?Y/CN36AuDa7ErZ0pxCmHLZCkPY7gVxXHxZzzutveXf1RQS6Hf7NAupyYCPeY?=
 =?us-ascii?Q?HmGY1PQ3gwkHwX3t3XbZ/aCx1zCjUDXjbBKuTg=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: BY5PR09MB4181
X-OrganizationHeadersPreserved: BY5PR09MB4181.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT007.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(7696005)(81166007)(9686003)(83080400001)(21480400003)(83380400001)(52536014)(89360
02)(19627405001)(1096003)(8676002)(55016002)(34756004)(186003)(356005)(2940100002)(8636
2001)(28085005)(26005)(6506007)(45080400002)(5660300002)(33656002)(109986005)(166002)(8
2310400002)(336012);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 5605d1a4-8015-4690-9cca-08d81cf6ae19
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-
ascii?Q?qCN/OrbfLFw1TLD4fUtbJtR3zc4VaK8OYxLhMbMHz3GmT61zCJIfwVhh+p4n?=
 =?us-ascii?Q?7jrMDTWBwllj+OON0nWfYqvKhwG3eN4IKihKl7A2H9QcBdwi0wI9Pa52hvrS?=
 =?us-ascii?Q?AQowuTWPTNt2GO+nRnBQUqn1AouBjCe3Tk8ZVncMxF9kgIkC3+RajxHMnORN?=
 =?us-ascii?Q?/yd7cG/QoLqgU2OAWyXEmqwxX0An7IyeGyjx7R1V5zMaQKsmvAGYLiNK8cEq?=
 =?us-ascii?Q?8Usu/XUPe7Mde8Kpj61ZVOJjujHw8CavjJCkw3PQFzYt3dZvlk5SdjwO8QJm?=
 =?us-ascii?Q?Joty7TM+omQ5UO9obKMTO/ZAFjhOilS8BQctBQJ8lslehrdKQ3mLCZu9s3M5?=
 =?us-ascii?Q?IEIGhoG+CJswXRVQ0XoEtJy904AKI9VffTfCoOX9I3YaV8Blsh/JB4h6YTqU?=
 =?us-ascii?Q?wI1Rat8LqLX7jM13SPFFJavDmO3aELmQNGiww0HyfpYfe/WL0sK3I56Gm4jF?=
 =?us-ascii?Q?nA/iohE2vosa9ie0p71xxYM85MlBldPVMY6LryUpO5IPb1ORFHuVSfals9sy?=
 =?us-ascii?Q?j68gNQmWeoETTjX2kkgt14e0+bnISzM56+IDDDyOdlX8MkEQlcuJe2eQj4WF?=
 =?us-ascii?Q?Pdzzuo3Nw+xPQSLKHgMYDFreYHWBbNzpH0fymHlO9ObJrxhreHT5tqH/yk0u?=
 =?us-ascii?Q?kYCEH5+WnYHxfQogsMX1GGBFJJXo6F76cYFWO8z50K3jTawDihUbCIEnyTqD?=
 =?us-ascii?Q?QfVWsseC0rmTD4CJvM7roKhs3DWoyynDGCabh7q+rhuzSMxsrGCC3SP/o5Ol?=
 =?us-ascii?Q?52VZZ++AJMJVjnvtrTADdoCBkHCkI7xOfm4jhtYlzgL+6jOOmaGGmnWw/i/L?=
 =?us-ascii?Q?cik4WOEWD25b+/PCOYg1aMW3tLqLCRY+QJPGfHi1lIzPDJTpOTqHp5q/jZOo?=
 =?us-ascii?Q?aeM00wBtyRdorHakfScwme9ZlJ+90qdnkwDYU7ppESYT5bW0+OQshyXk5pB5?=
 =?us-ascii?Q?+YD1uZhXjRiGnmUe6kUX5+fBRB706ABO05Fjn5fe89LL0qsXtZUm8oyGQfjj?=
 =?us-ascii?Q?37Vnxbofjw0BpE5Y4NM0fVfVhvMantuUoEqhcwc0yucHIx7so80M6cUrlRsH?=
 =?us-ascii?Q?Nok/WCEUN7hEKeEnAQgZtJL/DaohNHwXJYC9VMv5KV8T87AQBj+eP+uiqwxW?=
 =?us-ascii?Q?XQq6LlO7srf9hpWWQzf4wCUo6MYC7ho+YRJumrLbZ/y7G2H5s2tbkyumwoud?=
 =?us-ascii?Q?D5Ly+xxa0N4frxN5jI7Jy4//Ht6OsXP+kd1tZg=3D=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: MW2PR0901MB3819
X-OrganizationHeadersPreserved: MW2PR0901MB3819.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV02.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT008.eop-
gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-
1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV02.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;
SFS:(5660300002)(2940100002)(336012)(52536014)(26005)(6506007)(186003)(86362001)(968600
3)(19627405001)(33656002)(55016002)(45080400002)(8676002)(8936002)(1096003)(109986005)(
```

82310400002)(83380400001)(7696005)(81166007)(166002)(28085005)(34756004)(83080400001)(21480400003);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: b470eb5f-28c4-417f-f28c-08d81cf6d76b
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-ascii?Q?T3hKtGIx9hSul2OZTKGNj0VS+etWppUeboTni+IPjpGR9mjDvYgVJo4B6aV3?=
 =?us-ascii?Q?3FOMSM9TXGI6YUsK/9+y1Wv8C9JYdjrVUGkhoaoD1QHrELobinkVjWyvWBkX?=
 =?us-ascii?Q?dJ3WaPrXrcb9dncJABdyZthCOvQT9YQfmDMum2WGRSTfh4sF79N9OxVbw2hs?=
 =?us-ascii?Q?/EfnO+GAkeNkoG0iryqyJ6MMRM29uXtPRgEh4LCMZ98FP4Hep13juSTxTUho?=
 =?us-ascii?Q?Wg56s7O8aj27vItGGTI72hFgUCh4aqSArmZ3hNul/QWP1q8mIaKANL1Bv7TP?=
 =?us-ascii?Q?otc60leB9pJet1cUJXAdrpVE8wcBVKiyhqLMrbwUV7+kiQyq/dWQE2PQeOed?=
 =?us-ascii?Q?sMU864BYdoapxkZ9VkzCvqNDuCTyxwAe9Sh8u1CrdbUZb/YB3uRFTVSpVsdp?=
 =?us-ascii?Q?EB04wtrZDhp5whWU8tvkz9YiS0LfTAH7ntVD7QRuCZORxslAj/GAY7XjCcbs?=
 =?us-ascii?Q?tqkGK9sFcyJO0CR8pYQ3WbjoTxlgG6AuBsCwKoQlATxHikYl4rzZY06uGP5m?=
 =?us-ascii?Q?3Oe3phZ/RTHKZhZ985N5Agfv8G5zzovLJOVvuqBA5ZxJlDa78EnqOVWo0IZ1?=
 =?us-ascii?Q?8WwCX78n2PY52h5zDaTmJ/nLeToNWWWQDcvuzJ1pYgLdpLWPIKnJ9soPVeAx?=
 =?us-ascii?Q?hZ1+RgANyZJ/2J7AsZFOU3EKyEBvaUt//43B95q5LrTS/eZm+IBAgkPqSCQJ?=
 =?us-ascii?Q?KWw9+rrEY2kVdZregsOfF3bWbiNZ3mTfUTbBYerfOzh6iqW2CcNO98EsNr7F?=
 =?us-ascii?Q?wc+ulHqVPTTuWwnGV9DRTvo5Fnq3k9ppRLOr9yAgKzcY3vnji5NTlmWvSH4q?=
 =?us-ascii?Q?9XLRJX2elLyIfNlcWa461UaPPFhC+BAYOu9ZcKVVBIMXuNjSK0K6/mPnXCM4?=
 =?us-ascii?Q?09ErlNwkKJs6kMRKzoTL+qW3jZMY6gJ76fqCo6Ajg4oq6mlyFXyg2rzpLeQb?=
 =?us-ascii?Q?Qk+JdA7DNBBWHE1ThC2tzAK9Y3r96/HLDbM18T2MMnUHQE2xfHbjoWfe7FqD?=
 =?us-ascii?Q?MxR82BaCIE9kSPYB8Fxa695QL/jv7+HyGtCE3mfcWhPGC8M=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: SA9PR09MB5439
X-OrganizationHeadersPreserved: SA9PR09MB5439.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DM2GCC01FT007.eop-gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report-Untrusted: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;SFS:(26005)(5660300002)(109986005)(45080400002)(6506007)(52536014)(86362001)(356005)(81166007)(19627405001)(82310400002)(33656002)(9686003)(34756004)(7696005)(28085005)(55016002)(83380400001)(8676002)(336012)(186003)(1096003)(2940100002)(166002)(83080400001)(8936002)(21480400003);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: d16e5075-aa86-403a-675c-08d81cf8fad1
X-Microsoft-Antispam-Untrusted: BCL:0;
X-Microsoft-Antispam-Message-Info-Original: =?us-ascii?Q?IglXY3KuW8S9y9/wztnHgRPyMs4iEDSNkiWI3y7xHxVo93hiyXGpfRjPA3td?=
 =?us-ascii?Q?nus1IQW1UDlpNZQgfv1zysXujc8GtvQD+zk8OnLEHqNhSs95kxh+o5pQdVVZ?=
 =?us-ascii?Q?5AvK8mdphwny07TPF9AeG514vkZ6D6VTMo/1wiTJJpvXC1kFo7ExZf6wcTWX?=
 =?us-ascii?Q?RrIpzzF8wDGEvkWgo0XPez2Wq8g7IWoDY//vXUtuMrXhFeiEXK4rvToms8IM?=
 =?us-ascii?Q?ci3/erOWDE73YnUOYSdf0i10k1lOL+r20G2gNgHBhmNUIDd6hGRKdpe3RPeY?=
 =?us-ascii?Q?fUP5oc6WJ9+9ooAyAODtAdSU1WM0/H06hP28VI/6LFuuBICCqELMCp/WlOVk?=
 =?us-ascii?Q?ROUq/2RrMa3q0G1/TtkdldfjPkc8WQefUA/vGn8IsAvSYd0hltWvtWDInceI?=
 =?us-ascii?Q?DBGWlvgqkfeHjWhzs50bD1sdb18bk0CzIwZiPPo2fvk+uv10MHrgyfn1SFAh?=
 =?us-ascii?Q?pwsJEqNVSmXO0m5q4K+y2K4XTGqt33S/yoAb6v1QlHloyxv58Ikgjfoi/5Ax?=
 =?us-ascii?Q?0gaAhu8fKq4xF107tRPaWGk5a6YfscqtMa7B7m5GTl45xFKoJ16KKiZsn1S7?=
 =?us-ascii?Q?1bWsuiksA/xHawumVOp/CQdyNL+ZvU+T6hGF0FEMwEGGdoW7VxZRWcd/2n3n?=
 =?us-ascii?Q?adzvqo1+v82eGD7diXungpNNAJnKSam5edriVT7kIOftC9iOhVY0ATQybRwW?=
 =?us-ascii?Q?sE5afED2GXCXgnjXt5i2UDwl0zUVNw62RoN43bu2MkKnNpDtvvGbctpMTvGt?=
 =?us-ascii?Q?iyY8PWrTI0KuSLSuKafWfslIAf/7S8HlHdlirgJQTRvghMlsWg+p47m0sorH?=
 =?us-ascii?Q?DzvkhS6FdjUs7zGw/bjlSWjR5Tbqgj6rpeH9X1YU8R1FKSC7MQ95uRIEhBfs?=
 =?us-ascii?Q?DS08UKWrHxCpiuRneDw5zIYh+Nzv6XsUPvAI4xa7o5IO4TdCYhhvL3Yl7xDD?=
 =?us-ascii?Q?fKfvnEF4uPF4B2MDw+d13uZBV5gtiPpG9LlfuFTdS66F6JEUFnjdcSagHC0T?=
 =?us-ascii?Q?ERrnrFXpeD0zvCQTPtDxmu3eBORUhwneQAoWMEzelppU59s=3D?=
X-MS-Exchange-Transport-CrossTenantHeadersStamped: BY5PR09MB3873
X-OrganizationHeadersPreserved: BY5PR09MB3873.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-CrossPremisesHeadersFilteredBySendConnector: CCCASV01.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-MS-Exchange-Transport-CrossTenantHeadersStripped: CY1GCC01FT010.eop-gcc01.prod.protection.outlook.com
X-Forefront-Antispam-Report: CIP:162.217.184.79;CTRY:US;LANG:en;SCL:-1;SRV:;IPV:CAL;SFV:SKN;H:CCCASV01.CCOUNTY.com;PTR:InfoDomainNonexistent;CAT:NONE;SFTY:;SFS:(82310400002)(52536014)(45080400002)(83080400001)(186003)(166002)(336012)(214804000

03)(7696005)(26005)(6506007)(33656002)(81166007)(356005)(1096003)(5660300002)(196274050
01)(8676002)(2940100002)(9686003)(34756004)(28085005)(8936002)(55016002)(109986005)(833
80400001)(86362001);DIR:INB;SFP:;
X-MS-Office365-Filtering-Correlation-Id-Prvs: 5d14c9be-9361-48a6-1567-08d81cf9103c
X-Microsoft-Antispam: BCL:0;
X-Microsoft-Antispam-Message-Info: =?Windows-
1252?Q?fCw9VhR2VvpATVLZy94yoopgjeHvLIGoycDBT26I+u2Psoc9l7DUwRW/?=
 =?Windows-1252?Q?uZGAvccy0Dt5KyvefBfN5ktQ7AJg3UCqfdpPDxOSBGjBO2nZRc6a4Sck?=
 =?Windows-1252?Q?nEhC4mbwaTcFyzHIjKINizpM54lEUydvBOjTFBnSNBMOq5bYnHUyWwUz?=
 =?Windows-1252?Q?iT0nG3FF+GW4p1GVLHRwU66MPHRvj/anqi9xYZo+GJcXTEYg80Cjyc/W?=
 =?Windows-1252?Q?7FAd4PbDpKNZV4zd+YjQwo8hcFTtb5i3mEQMA/bPBJaxwQ7vr8gqPoQl?=
 =?Windows-1252?Q?UetX+ahhp1akUzUGc4Z9XP7dGny/2tV6PaBZxTo1DuLsdQbn/MsqA4E3?=
 =?Windows-1252?Q?6gDMmOnISXFrBesq9TfhNqVRDJw2kZC8ijSs/1oE5hTtc9Nh0JS1/Q7R?=
 =?Windows-1252?Q?qjSrm/x+j1w6x2sdDZKQsur5t0wvvFhy/AO9/lHpI4YxqueZQYA4sDQA?=
 =?Windows-1252?Q?AuUP/CIq7VXcmcquWfWURQpDiLoldECejz4lAwvCzitCCCHRZq8EPkrX?=
 =?Windows-1252?Q?FmZnN/2rZ/cbmPJIasu8oI2MbDcSUrM3nvnQvXrdE5b6Zaza2mUlKhIs?=
 =?Windows-1252?Q?8hCbdk+rr3uzpxPxHXHiOxlq36IS0Oj196KDwl03X5tU2yI8slHRHrgA?=
 =?Windows-1252?Q?1zlwzdwQVedKLdTQA4ykOrp1WpKxqjxsKWC1nYwk/ESEPy1OgT5hQYVb?=
 =?Windows-1252?Q?zuorbXQUJoaqaZR3PktG0BbPyVJcdM8uJeHwB9sWmv8fkQ5EfYGIFroR?=
 =?Windows-1252?Q?CZmPqTrppYSSFuZgjeUmvxvqmzRcDl36h+U24fU6HR/Nk1Zr1uIzDnVv?=
 =?Windows-1252?Q?jHH7U1PEJQuG91/j9wMF/w0hvHt6JbtlKbZPnOYINFZYfRtTdJ4s8K78?=
 =?Windows-1252?Q?u40OOl18YZtGOg5F8W07ySdEEbNmWv/caAHjowc+//IIsbSGuiCUi4FA?=
 =?Windows-1252?Q?5FZzwOUjGqvCeSyNDO5zzvzO9oYNexlPP8oZsaqSldexscaY12l0nzZN?=
 =?Windows-1252?Q?VgDqZlcCdFQmE3QiyaBHnH8p7rijQpZO1blv/EkbB8wbjxIY4mPycsNQ?=
 =?Windows-1252?Q?JOugXmc8+0Soyv+4V74nB2/Vf4gMpOc8cSLLDViqC3Hz7J/0YOHS6zJe?=
 =?Windows-1252?Q?bVY=3D?=
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 30 Jun 2020 13:40:38.8976
 (UTC)
X-MS-Exchange-CrossTenant-Network-Message-Id: ae69832f-1896-462e-8066-08d81cfb2cf6
X-MS-Exchange-CrossTenant-Id: 8b4d55ae-6db4-4e05-a85c-59d6a256cd6e
X-MS-Exchange-CrossTenant-OriginalAttributedTenantConnectingIp: TenantId=8b4d55ae-6db4-
4e05-a85c-59d6a256cd6e;Ip=[162.217.184.79];Helo=[CCCASV01.CCOUNTY.com]
X-MS-Exchange-CrossTenant-AuthSource: CY1GCC01FT010.eop-
gcc01.prod.protection.outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Anonymous
X-MS-Exchange-CrossTenant-FromEntityHeader: HybridOnPrem
X-MS-Exchange-Transport-CrossTenantHeadersStamped: BYAPR09MB3189
X-OrganizationHeadersPreserved: BYAPR09MB3189.namprd09.prod.outlook.com
X-CrossPremisesHeadersFiltered: CCCASV02.CCOUNTY.com
X-OrganizationHeadersPreserved: CCCASV01.CCOUNTY.com
X-CrossPremisesHeadersFilteredByDsnGenerator: CCCASV01.CCOUNTY.com

Undeliverable: Pass Through - (U//FOUO) Criminal Hackers Target US Law Enforcement Data

To:	Eric.Sellers@cookcountyil.gov, Mary.Tamme@cookcountyil.gov, Wanda.Barnes@cookcountyil.gov, Vincent.Gamez@cookcountyil.gov, Thomas.Shader@cookcountyil.gov, Tangenise.Porter@cookcountyil.gov, Tamara.Levickas@cookcountyil.gov, Samuel.Cory@cookcountyil.gov, Ronald.Prohaska@cookcountyil.gov, Roger.Comer@cookcountyil.gov, Robert.Waller@cookcountyil.gov, Robert.O'Neill@cookcountyil.gov, Richard.Petersen@cookcountyil.gov, Rex.Knaperek@cookcountyil.gov, Paul.Riley@cookcountyil.gov, Paul.Huss@cookcountyil.gov, Nancy.Pavelka@cookcountyil.gov, Michael.Quan@cookcountyil.gov, Michael.Gomez@cookcountyil.gov, Michael.Anton@cookcountyil.gov, Maurice.Cernick@cookcountyil.gov, Matthew.Walsh@cookcountyil.gov, Alexander.Brodie@cookcountyil.gov, Lisa.Farinella@cookcountyil.gov, Kevin.Graff@cookcountyil.gov, Kevin.Cooper@cookcountyil.gov, Kevin.Christofidis@cookcountyil.gov, Kelly.Sweeney@cookcountyil.gov, Jonathan.Mobley@cookcountyil.gov, John.Steed@cookcountyil.gov, John.Pradun@cookcountyil.gov, Jeffrey.Pasqua@cookcountyil.gov, James.Scannell@cookcountyil.gov, James.Hughes@cookcountyil.gov, Lissette.Rivera@cookcountyil.gov, Giovanni.Veitkus@cookcountyil.gov, Gary.Newsom@cookcountyil.gov, Frank.Caridei@cookcountyil.gov, Felix.Arvelo@cookcountyil.gov, Diane.Haras@cookcountyil.gov, David.Delgado1@cookcountyil.gov, Daniel.Strong@cookcountyil.gov, Daniel.Burke@cookcountyil.gov, Cedric.Mccloud@cookcountyil.gov, Catherine.Domine@cookcountyil.gov, Anthony.Burns@cookcountyil.gov, Gary.Rizzo@cookcountyil.gov, Luis.Santoyo@cookcountyil.gov, Ricardo.Hardy@cookcountyil.gov, Wanda.Walker@cookcountyil.gov, William.Mak@cookcountyil.gov, Daniel.Moreci@cookcountyil.gov, Darren.Makowski@cookcountyil.gov, Dennis.Nicpan@cookcountyil.gov, James.Dillon@cookcountyil.gov, John.Hammond@cookcountyil.gov, Joseph.Giunta@cookcountyil.gov, Leonard.Jagielski@cookcountyil.gov, Miles.Cooperman@cookcountyil.gov, Patrick.Hecker@cookcountyil.gov, Richard.OBrien1@cookcountyil.gov, Richard.Young2@cookcountyil.gov, Joseph.Danzl@cookcountyil.gov, Zelda.Whittler@cookcountyil.gov, CCSO Intel (Sheriff)
Sent:	June 30, 2020 8:56:06 AM CDT
Received:	June 30, 2020 8:56:11 AM CDT

Anarchist Exremists/Criminal hackers

From:	Robert Lunk (Sheriff) <Robert.Lunk@cookcountyil.gov>
To:	Tarry Williams (Sheriff) <Tarry.Williams@cookcountyil.gov>, Kathleen Urbanczyk (Sheriff) <Kathleen.Urbanczyk@cookcountyil.gov>
Sent:	June 30, 2020 9:36:07 AM CDT
Received:	June 30, 2020 9:36:09 AM CDT
Attachments:	Anarchist Extremists - Antifa.pdf, (U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

Robert A. Lunk
Investigator #6236
Cook County Sheriff's Office
Cell (312) 343-4684
Robert.Lunk@cookccountyil.gov

THIS IS A CONFIDENTIAL LAW ENFORCEMENT COMMUNICATION. The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential. If you are not the intended recipient of this message, or if this message has been addressed to you in error, please immediately alert the sender by reply-email and then delete this message and its attachments. Do not deliver, distribute, transmit or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action relative to the information contained in this communication and/or attachments. This e-mail and any attached documents may contain Law Enforcement Sensitive material and should not be disseminated outside of official law enforcement channels. The information contained in this message as well as any attachments shall not be released to the media or the general public.

Anarchist Exremists/Criminal hackers

From:	Robert Lunk (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=AADABC964D1E4668A94B0C827FB7CBA0-ROBERT LUNK>
To:	Tarry Williams (Sheriff) <Tarry.Williams@cookcountyil.gov>, Kathleen Urbanczyk (Sheriff) <Kathleen.Urbanczyk@cookcountyil.gov>
Sent:	June 30, 2020 9:36:07 AM CDT
Received:	June 30, 2020 9:36:08 AM CDT
Attachments:	Anarchist Extremists - Antifa.pdf, (U--FOUO) IIB - Criminal Hackers Target US Law Enforcement Data 06262020.pdf

Robert A. Lunk
Investigator #6236
Cook County Sheriff's Office
Cell (312) 343-4684
Robert.Lunk@cookccountyil.gov

THIS IS A CONFIDENTIAL LAW ENFORCEMENT COMMUNICATION. The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential. If you are not the intended recipient of this message, or if this message has been addressed to you in error, please immediately alert the sender by reply-email and then delete this message and its attachments. Do not deliver, distribute, transmit or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action relative to the information contained in this communication and/or attachments. This e-mail and any attached documents may contain Law Enforcement Sensitive material and should not be disseminated outside of official law enforcement channels. The information contained in this message as well as any attachments shall not be released to the media or the general public.

Anarchist Exremists/Criminal hackers

To:	Tarry Williams (Sheriff), Kathleen Urbanczyk (Sheriff)
Sent:	June 30, 2020 9:36:07 AM CDT
Received:	June 30, 2020 9:36:08 AM CDT

FW: (U/LES) TAM-C Situation Report United States: 30 June 2020 #2

From:	Thomas Tilton (Emergency Management) <Thomas.Tilton@cookcountyil.gov>
To:	Michael Brady (Sheriff) <Michael.Brady@cookcountyil.gov>, Robert Lunk (Sheriff) <Robert.Lunk@cookcountyil.gov>
Sent:	June 30, 2020 12:17:06 PM CDT
Received:	June 30, 2020 12:17:14 PM CDT
Attachments:	TAM-C Situation Report United States_ 30 June 2020 #2.xlsx, DHS IG Report on UAS June 2020.pdf, 2020_06_30.pdf, DMWF200630.pdf, Coronavirus Special OSINT Report - SOR 103-20.pdf

FYI

From: Ness, Michael <michael.ness@hq.dhs.gov>
Sent: Tuesday, June 30, 2020 11:54 AM
To: Adrian Cunningham (Adrian.Cunningham@fema.dhs.gov); 'Adrianne.Michele@socom.mil'; AITES, KELLIE A CIV USAF ACC 55 SFS/S5AT <kellie.aites@us.af.mil>; 'Allen_Rothbaum@ios.doi.gov'; Anderson, Matthew E LT USN STRATCOM J34 (USA) (matthew.e.anderson5.mil@mail.mil) <matthew.e.anderson5.mil@mail.mil>; Distler, Andrew (CTR) <andrew.distler@associates.hq.dhs.gov>; MARCUS, ANDREW <andrew.marcus@hq.dhs.gov>; Anna Castillo <anna.castillo.1@us.af.mil>; Brad Tippit (Brad.Tippit@Missouricitytx.gov) <Brad.Tippit@Missouricitytx.gov>; 'Bruce.Steven.Miller@us.army.mil'; Pelton, Bryan (CTR) <bryan.pelton@associates.hq.dhs.gov>; 'captain@berwickpolice.org'; Chandra White <Chandra.white@us.af.mil>; Oppliger, Christopher <christopher.oppliger@hq.dhs.gov>; Cisneros, Tony <Tony.Cisneros@fletc.dhs.gov>; 'CLTibbs@co.pg.md.us'; ALFORD, DALE <dale.alford@hq.dhs.gov>; 'Darryl_Ward@ios.doi.gov'; ATWOOD, DAVID (CTR) <david.atwood@associates.hq.dhs.gov>; Davidson, Jeffrey <jeffrey.davidson@hq.dhs.gov>; Delcore, Robert <Robert.Delcore@uscis.dhs.gov>; Delgado, Jose L <Jose.Delgado@tsa.dhs.gov>; 'dennis.gonzalez@CityofRochester.gov'; dgirou@arlingtonva.us; 'dgpeterson@lanl.gov'; Schwarzrock, Don <don.schwarzrock@hq.dhs.gov>; Downey, Michael <Michael.Downey@hq.dhs.gov>; Dzurilla, Christopher <Christopher.Dzurilla@HQ.DHS.GOV>; Gagnon, Bruce P <Bruce_Gagnon@nps.gov>; Graves, Jeremy W MSgt USAF AFDW (USA) (jeremy.w.graves.mil@mail.mil) <jeremy.w.graves.mil@mail.mil>; greg.brock@nlrb.gov; HARDING, DANIEL <daniel.harding@hq.dhs.gov>; Harvey, Timothy <Timothy.Harvey@fletc.dhs.gov>; Henry Rivero: <Henry.Rivero@bep.gov>; 'hhgreen@nmic.navy.mil'; Holder, Richard <Richard.Holder@HQ.DHS.GOV>; Hughes, Gregory (CDC/OPHSS/NCHS) (nvx2@cdc.gov) <nvx2@cdc.gov>; Hunter, Joseph David (Joe) 2d LT USAF (US) (joseph.d.hunter16.mil@mail.mil) <joseph.d.hunter16.mil@mail.mil>; CURRIE, JASON (CTR) <jason.currie@associates.hq.dhs.gov>; Jeffrey McClung <jeffrey.mcclung@jfcc-imd.stratcom.mil>; Henderson, Jesse K CTR <Jesse.K.Henderson@uscg.mil>; Tadrick, Joe <Joe.Tadrick@hq.dhs.gov>; John Bamford <Jbamford@arlingtonva.us>; 'john.a.kavaliunas.civ@mail.mil'; 'John.Glodo@crystal.dia.mil'; 'john.leo-1@nasa.gov'; Jonesmcgee, Darius A SSgt USAF (USA) (darius.a.jonesmcgee.mil@mail.mil) <darius.a.jonesmcgee.mil@mail.mil>; JS Pentagon DoM Mailbox JSSO Military Security Force <js.pentagon.dom.mbx.jsso-military-security-force@mail.mil>; kenneth.j.anderson3.civ@mail.mil; Kristy KorchakCampbell (kristy.korchakcampbell@us.af.mil) <kristy.korchakcampbell@us.af.mil>; kristy.korchak-campbell@auab.afcent.af.mil; 'kunichs@guestservices.com'; Battiste, Lawrence <lawrence.battiste@hq.dhs.gov>; Lee Taylor (Lee.Taylor@hq.dhs.gov); Linneman, Eric <Eric.linneman@dla.mil>; Mannix, Alan <Alan.Mannix@bep.gov>; 'mark.holloway@ic.fbi.gov'; Marler, Christopher F SSgt USAF (USA) (christopher.f.marler.mil@mail.mil) <christopher.f.marler.mil@mail.mil>; Mascolo, John <John.Mascolo@tsa.dhs.gov>; 'Matthew.f.croson@usdoj.gov'; McBride, Chip <chip.mcbride@hq.dhs.gov>; Michael Malcolm <michael.s.malcolm2.civ@mail.mil>; Michael Robinson: <michael.robinson@bep.gov>; 'michael.g.copeland2.civ@mail.mil'; Michael.Kenny@bep.gov; 'michael.w.young8.ctr@mail.mil'; Mike Evans <Mike.Evans@calvertcountymd.gov>; monika.l.junker.civ@mail.mil; Moreta, Richard <richard.moreta@hq.dhs.gov>; Nicholas Paoletti (nicholas.paoletti.1@us.af.mil) <nicholas.paoletti.1@us.af.mil>; 'n-nc.peterson.ncj3.mbx.j34-letic-omb@mail.mil'; 'Odis.Stroud@cookcountyil.gov'; Oppermann, George Henry CIV USARMY USAG (US) <george.h.oppermann.civ@mail.mil>; Ortega, John A CIV <John.A.Ortega@uscg.mil>; Booker, Patrick M (N/A) <patrick.m.booker@uscis.dhs.gov>; Patterson, Richard V (Rick) CTR STRATCOM J34 (US) <richard.v.patterson.ctr@mail.mil>; Pepin, Andrew <Andrew.Pepin@HQ.DHS.GOV>; Groven, Philip <Philip.Groven@hq.dhs.gov>; Ping, William Darion <william.d.ping.civ@mail.mil>; Pinkham, Lawrence H JR CIV STRATCOM J34 (US) <lawrence.h.pinkham.civ@mail.mil>; 'PittmanT@state.gov'; POULSEN, ROBERT A 2d Lt USAF ACC 55 ISS/IN <robert.poulsen@us.af.mil>; 'Raymond.Hankins@nlrb.gov'; Loveless, Richard

<richard.loveless@hq.dhs.gov>; Richard Reed <Richard.Reed@firstnet.gov>; Richard Swarens <Richard.Swarens@whmo.mil>; 'Richard.Cestero@bep.gov'; Roddy, Gene E. CIV WHMO/HQ <Gene.E.Roddy@whmo.mil>; Russell, John W MSG USARMY JS DOM (US) <john.w.russell36.mil@mail.mil>; 'russell.r.hicks.civ@mail.mil'; BOYER, RYAN <ryan.boyer@hq.dhs.gov>; 'Ryan.Gibson@faa.gov'; 'Salvatore.ingraldi.civ@mail.mil'; Shell, Alvin <alvin.shell@bep.gov>; Sims, Karen <karen.sims@hq.doe.gov>; 'smithbr@state.gov'; Stephen J Barbieri (stephen.j.barbieri@uscis.dhs.gov); Stephen Kunich <Stephen.Kunich@pae.com>; 'Stephen.Hutchens@bep.gov'; Steven Schoen <steven.m.schoen@lmco.com>; Stewart, Kerry <Kerry.Stewart@cisa.dhs.gov>; Stewart, Kevin L CTR <Kevin.L.Stewart@uscg.mil>; 'sylvia.c.harris.civ@mail.mil'; Thomas Klug: <Thomas.Klug@bep.gov>; 'thomas.a.stroud@nasa.gov'; 'thomas.loyd@uscp.gov'; 'Thomas.Tilton@cookcountyil.gov'; Torian, William A Jr CIV USAF (USA) (william.a.torian.civ@mail.mil) <william.a.torian.civ@mail.mil>; Versichelli, Thomas <thomas.versichelli.civ@mail.mil>; Victor Calloway <vcalloway@gpo.gov>; Waage, Timothy S CIV STRATCOM J34 (US) <timothy.s.waage.civ@mail.mil>; Waterman, Ronald T CIV DSS DSS ISFO (US) <ronald.t.waterman.civ@mail.mil>; BERG, WENDY <wendy.berg@hq.dhs.gov>; WERNER, MATTHEW R TSgt USAF AFOSI 55 SFS/Det 204 <matthew.werner.4@us.af.mil>; Wilemon, Nicole <nwilemon@blm.gov>; DeArcangelis, William <william.dearcangelis@HQ.DHS.GOV>; Balcerzak, William J <William.J.Balcerzak@uscis.dhs.gov>; Wilson, Randall Craig CIV USARMY 21 SIG BDE (USA) (randall.c.wilson12.civ@mail.mil) <randall.c.wilson12.civ@mail.mil>; Wolf, Thomas John (Tom) CIV USARMY 21 SIG BDE (US) (thomas.j.wolf.civ@mail.mil) <thomas.j.wolf.civ@mail.mil>; Wyman, Isabel <isabel.wyman@hq.dhs.gov>
Subject: FW: (U/LES) TAM-C Situation Report United States: 30 June 2020 #2

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Michael "Elliot" Ness
Program Manager
Industrial Security Branch – CCIPP Program Office
Office of Chief Security Officer | National Security Services Division |
DHS-HQ Desk: 202-447-5046 | Mobile Work Cell: 202-853-0569
Email(s): michael.ness@hq.dhs.gov, or OCSO-SARM@hq.dhs.gov

Homeland Security

"With honor and integrity, we will safeguard the American people, our homeland, and our values."

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator. This communication, along with any attachments, is covered by Federal and State law governing electronic communications and may contain restricted and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message.

From: McIntyre, Timothy A <Timothy.A.McIntyre@ice.dhs.gov>
Sent: Tuesday, June 30, 2020 11:08 AM
To: Ness, Michael <michael.ness@hq.dhs.gov>
Subject: (U/LES) TAM-C Situation Report United States: 30 June 2020 #2

Please see below identified upcoming events throughout the United States in connection to the death of George Floyd in Minneapolis on 25 May 2020.

Region	City	Date	Time (Local Time)	Lat	Lng	Details
California	Sacramento	7/1/2020	11:30LT	38.576588	-121.493258	On 1 July 2020, at 11:30LT, activists in Sacramento, CA plan to gather at the California State Capital (38.576588, -121.493258).
California	San Jose	7/2/2020	14:00LT	37.337936	-121.884959	On 2 July 2020, at 14:00LT, activists in San Jose, CA plan to gather at the San Jose City Hall (37.337936, -121.884959) and will march trough Highway 101.
California	San Rafael	7/3/2020	17:00LT	37.998162	-122.530775	On 3 July 2020, at 17:00LT, activists in San Rafael, Marin County, CA plan to gather at at the Marin County Jail, located at 13 Peter Behr Drive (37.998162, -122.530775).
California	Santa Clara	7/3/2020	14:00LT	37.342293	-121.974469	On 3 July 2020, at 14:00LT, activsts in Santa Clara, CA plan to gather at Adrian Wilcox High School (37.366277, -121.986160) and will march to Central Park

						(37.342293, -121.974469).
North Carolina	Wilmington	7/1/2020	17:00LT	34.237058	-77.945888	On 1 July 2020, at 17:00LT, activists in Wilmington, NC plan to gather at 102 North 3rd Street (34.237058, -77.945888).
Pennsylvania	Allentown	7/1/2020	15:30LT	40.597757	-75.488056	On 1 July 2020, at 15:30LT, activists in Allentown, PA plan to gather at the corner of 15th Street and Hamilton Street (40.597757, -75.488056).
Texas	Dallas	7/1/2020	18:00LT	32.776428	-96.797088	On 1 July 2020, at 18:00LT, activists in Dallas, TX, will stage a protest in front of the City Hall (32.776428, -96.797088).
Texas	Denton	7/1/2020	14:00LT and 18:00LT	33.215034	-97.132987	On 1 July 2020, at 14:00LT and 18:00LT, activists in Denton, TX plan to hold two protests at Courthouse-on-the-Square Museum (33.215034, -97.132987).
Virginia	Fredericksburg	7/1/2020	16:00LT	38.301723	-77.462895	On 1 July 2020, at 16:00LT, activists in Fredericksburg, VA plan to gather at Hurkamp Park

						(38.301723, -77.462895).

TAM-C Operations
operations@tamcintel.com
24/7: +1.202.922.0068
https://www.tamc365.com/

This email transmission and any accompanying attachments may contain TAM-C Solutions privileged and confidential information intended only for the use of the intended addressee. Any dissemination, distribution, copying or action taken in reliance on the contents of this email by anyone other than the intended recipient is strictly prohibited. If you have received this email in error please immediately delete it and notify sender at the above TAM-C Solutions email address. Sender and TAM-C Solutions accept no liability for any damage caused directly or indirectly by receipt of this email.

UNCLASSIFIED//FOR OFFICIAL USE ONLY//HSIN Intelligence Community Distribution

To:	Abraham Yasin (Sheriff) <Abraham.Yasin@cookcountyil.gov>, Tarry Williams (Sheriff) <Tarry.Williams@cookcountyil.gov>, Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov>, Adriana Morales (Sheriff) <Adriana.Morales@cookcountyil.gov>, Alfonzo Hunter (Sheriff) <Alfonzo.Hunter@cookcountyil.gov>, Amanda Gallegos (Sheriff) <Amanda.Gallegos@cookcountyil.gov>, Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Bradley Curry (Sheriff) <Bradley.Curry@cookcountyil.gov>, Brian White (Sheriff) <Brian.White@cookcountyil.gov>, Carmen Gercone (Sheriff) <Carmen.Gercone@cookcountyil.gov>, Carmen Ruffin (Sheriff) <Carmen.Ruffin@cookcountyil.gov>, Christopher Imhof (Sheriff) <Christopher.Imhof@cookcountyil.gov>, David Chiko (Sheriff) <David.Chiko@cookcountyil.gov>, Erik Roedel (Sheriff) <Erik.Roedel@cookcountyil.gov>, Gregory Ernst (Sheriff) <Gregory.Ernst@cookcountyil.gov>, Heather Bock (Sheriff) <Heather.Bock@cookcountyil.gov>, Jennifer Black (Sheriff) <Jennifer.Black@cookcountyil.gov>, Jerry Baldwin (Sheriff) <Jerry.Baldwin@cookcountyil.gov>, John Vega (Sheriff) <John.Vega@cookcountyil.gov>, John Webb (Sheriff) <John.Webb@cookcountyil.gov>, Jonathan Myslinski (Sheriff) <Jonathan.Myslinski@cookcountyil.gov>, Joseph Bellettiere (Sheriff) <Joseph.Bellettiere@cookcountyil.gov>, Kathleen Urbanczyk (Sheriff) <Kathleen.Urbanczyk@cookcountyil.gov>, Kelley Eldridge (Sheriff) <Kelley.Eldridge@cookcountyil.gov>, Kevin Connelly (Sheriff) <Kevin.Connelly@cookcountyil.gov>, Kevin Ruel (Sheriff) <Kevin.Ruel@cookcountyil.gov>, Larry Schurig (Sheriff) <Larry.Schurig@cookcountyil.gov>, Lonnie Hollis (Sheriff) <Lonnie.Hollis@cookcountyil.gov>, Marlon Parks (Sheriff) <Marlon.Parks@cookcountyil.gov>, Matthew Creen (Sheriff) <Matthew.Creen@cookcountyil.gov>, Michael Brady (Sheriff) <Michael.Brady@cookcountyil.gov>, Michael Lucente (Sheriff) <Michael.Lucente@cookcountyil.gov>, Michael Miller (Sheriff) <Michael.Miller1@cookcountyil.gov>, Patrick Dwyer (Sheriff) <Patrick.Dwyer@cookcountyil.gov>, Patrick Moerlien (Sheriff) <Patrick.Moerlien@cookcountyil.gov>, Richard Brogan (Sheriff) <Richard.Brogan@cookcountyil.gov>, Richard O'Brien (Sheriff) <richard.obrien2@cookcountyil.gov>, Robert Lunk (Sheriff) <Robert.Lunk@cookcountyil.gov>, Ronald Jenkins (Sheriff) <Ronald.Jenkins@cookcountyil.gov>, Stephen Bouffard (Sheriff) <Stephen.Bouffard@cookcountyil.gov>, Theodore Stajura (Sheriff) <Theodore.Stajura@cookcountyil.gov>, Jason Hernandez (Sheriff) <Jason.Hernandez@cookcountyil.gov>, James Moore (Sheriff) <James.Moore2@cookcountyil.gov>
Sent:	June 30, 2020 4:34:00 PM CDT
Received:	June 30, 2020 4:33:38 PM CDT
Attachments:	SIN06292020 (U) July 2020 Dates of Significance.pdf, OSIR-04001-0809-20.pdf, OSIR-04001-0808-20.pdf

ALLCON:

Please see attached latest intelligence bulletins from the HSIN Intelligence Community.

Jasmine Adams

Criminal Research Analyst II

Cook County Sheriff's Department

Strategic Operations Center

3026 S California Ave.

Bldg.. 5, 2nd Floor Rm 205

Chicago, Illinois 60608

Email: ***jasmine.adams@cookcountyil.gov***

Distribution

To:	Abraham Yasin (Sheriff), Tarry Williams (Sheriff), Leo Schmitz (Sheriff), Adriana Morales (Sheriff), Alfonzo Hunter (Sheriff), Amanda Gallegos (Sheriff), Amar Patel (Sheriff), Bradley Curry (Sheriff), Brian White (Sheriff), Carmen Gercone (Sheriff), Carmen Ruffin (Sheriff), Christopher Imhof (Sheriff), David Chiko (Sheriff), Erik Roedel (Sheriff), Gregory Ernst (Sheriff), Heather Bock (Sheriff), Jennifer Black (Sheriff), Jerry Baldwin (Sheriff), John Vega (Sheriff), John Webb (Sheriff), Jonathan Myslinski (Sheriff), Joseph Bellettiere (Sheriff), Kathleen Urbanczyk (Sheriff), Kelley Eldridge (Sheriff), Kevin Connelly (Sheriff), Kevin Ruel (Sheriff), Larry Schurig (Sheriff), Lonnie Hollis (Sheriff), Marlon Parks (Sheriff), Matthew Creen (Sheriff), Michael Brady (Sheriff), Michael Lucente (Sheriff), Michael Miller (Sheriff), Patrick Dwyer (Sheriff), Patrick Moerlien (Sheriff), Richard Brogan (Sheriff), Richard O'Brien (Sheriff), Robert Lunk (Sheriff), Ronald Jenkins (Sheriff), Stephen Bouffard (Sheriff), Theodore Stajura (Sheriff), Jason Hernandez (Sheriff), James Moore (Sheriff)
Sent:	June 30, 2020 4:34:00 PM CDT
Received:	June 30, 2020 4:33:38 PM CDT

New courses available!

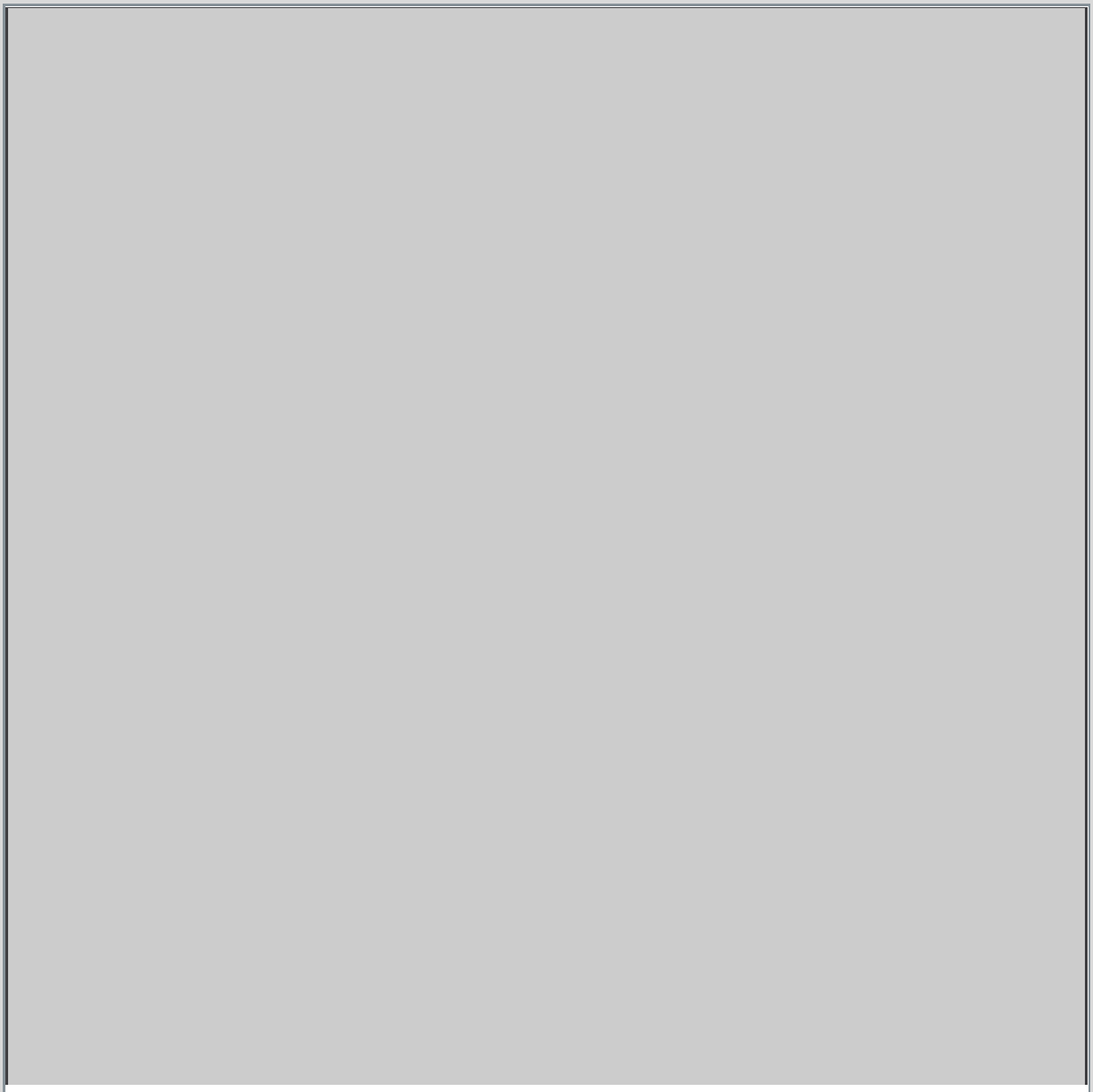
From: NW3C <training@nw3c.org>
To: terrence.doran@cookcountyil.gov, Terrence Doran (Sheriff) <Terrence.Doran@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:03 PM CDT
Received: June 30, 2020 11:10:09 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

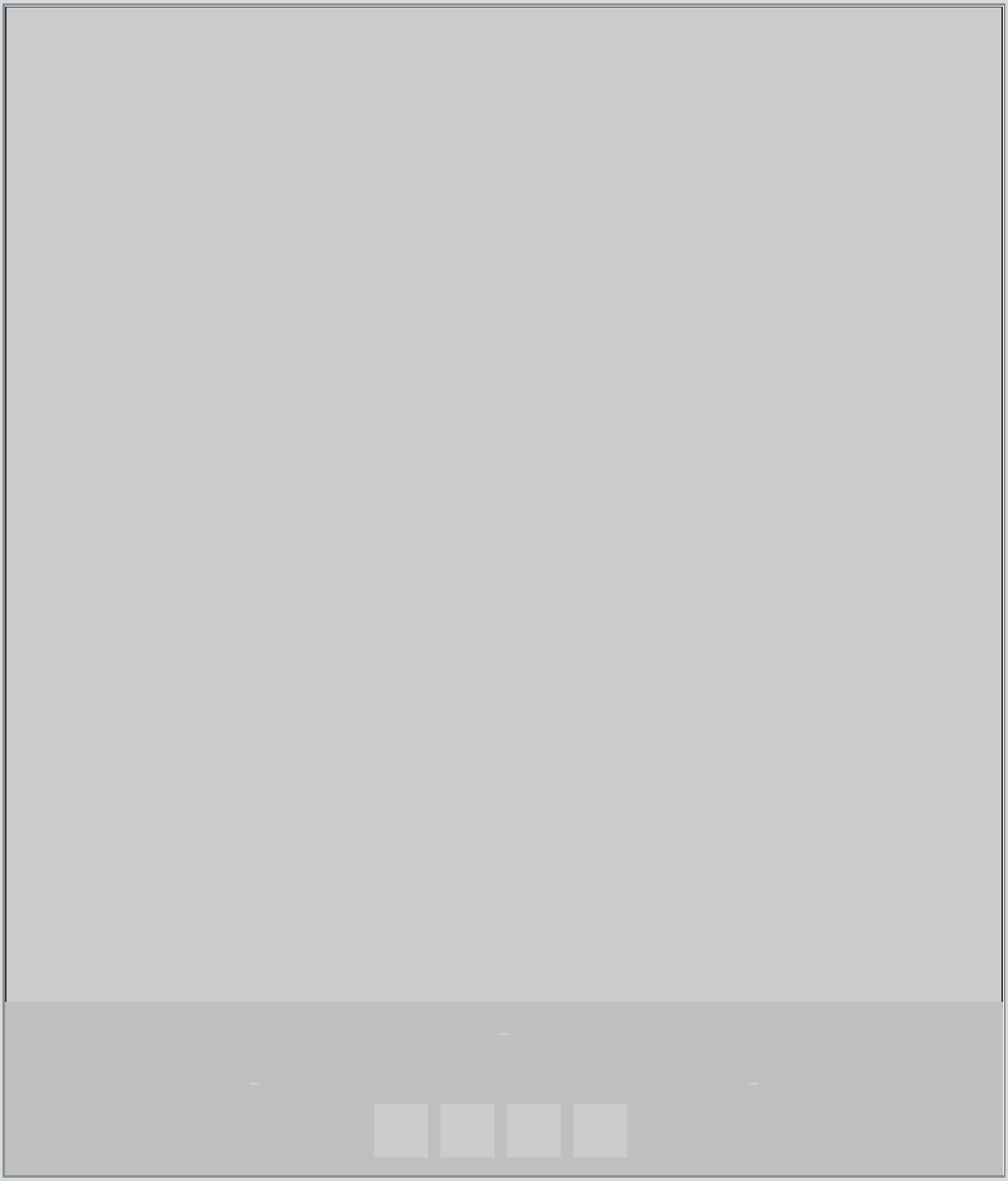
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

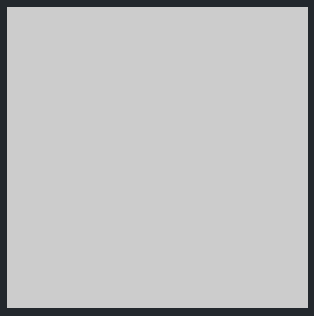
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

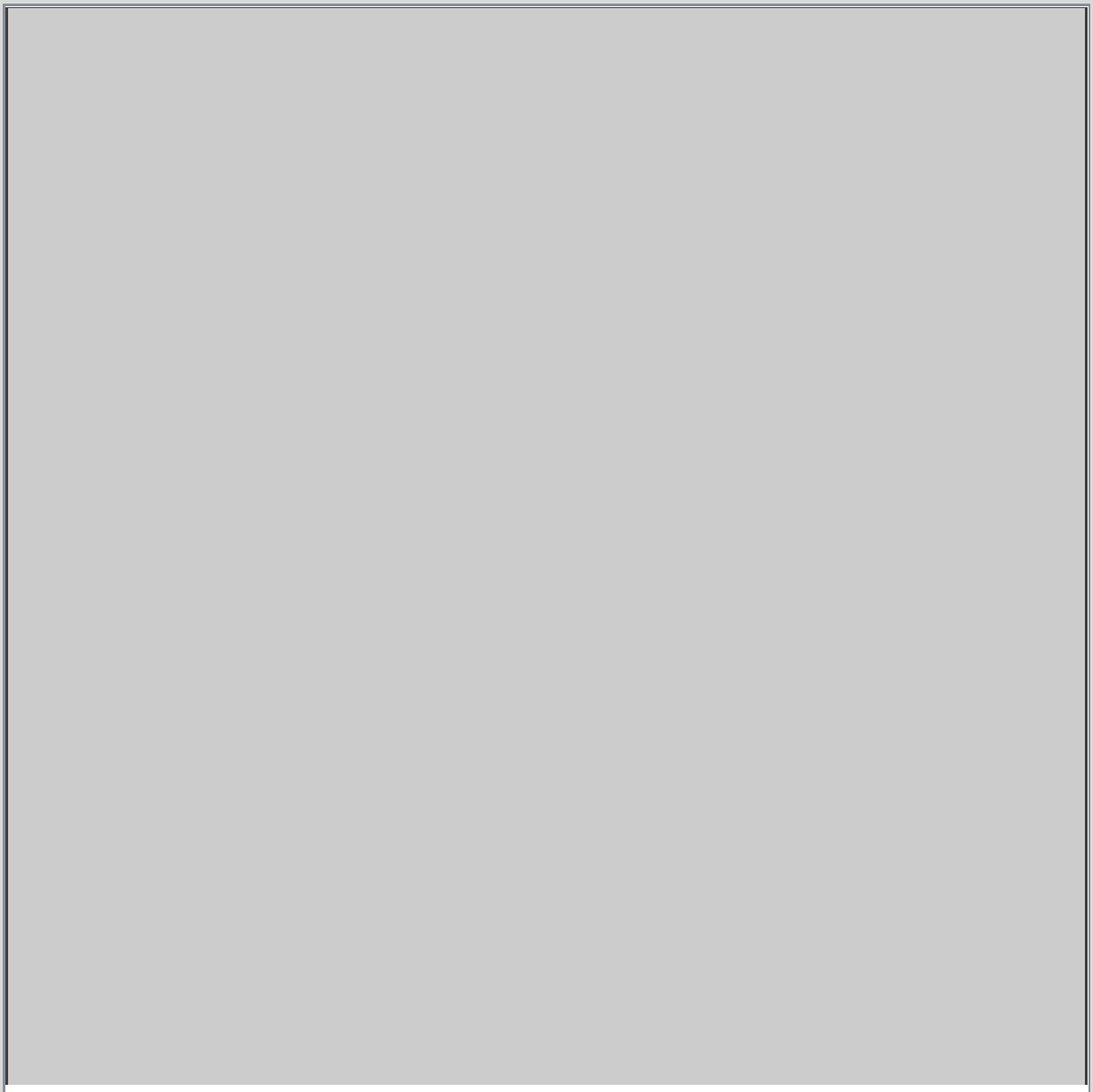
From: NW3C <training@nw3c.org>
To: fontella.brown-marshall@cookcountyil.gov, Fontella BrownMarshall (Sheriff) <fontella.brownmarshall@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:03 PM CDT
Received: June 30, 2020 11:10:07 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

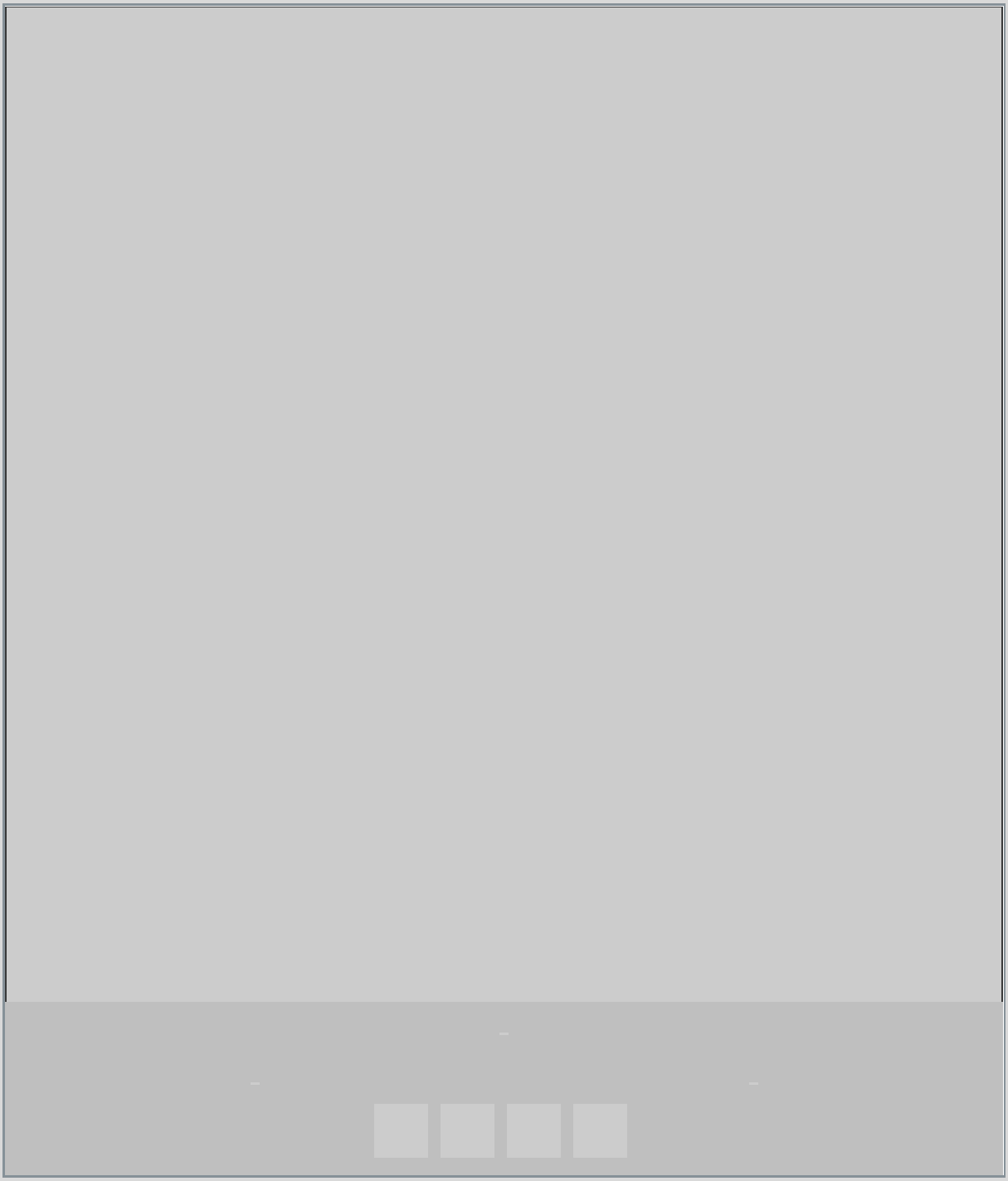
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

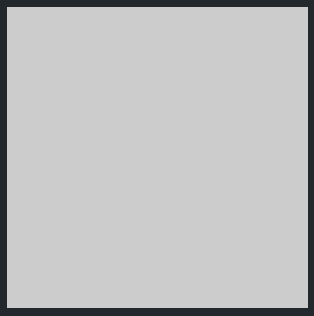
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Terrence Doran (Sheriff)
Sent:	June 30, 2020 11:10:03 PM CDT
Received:	June 30, 2020 11:10:10 PM CDT

New courses available!

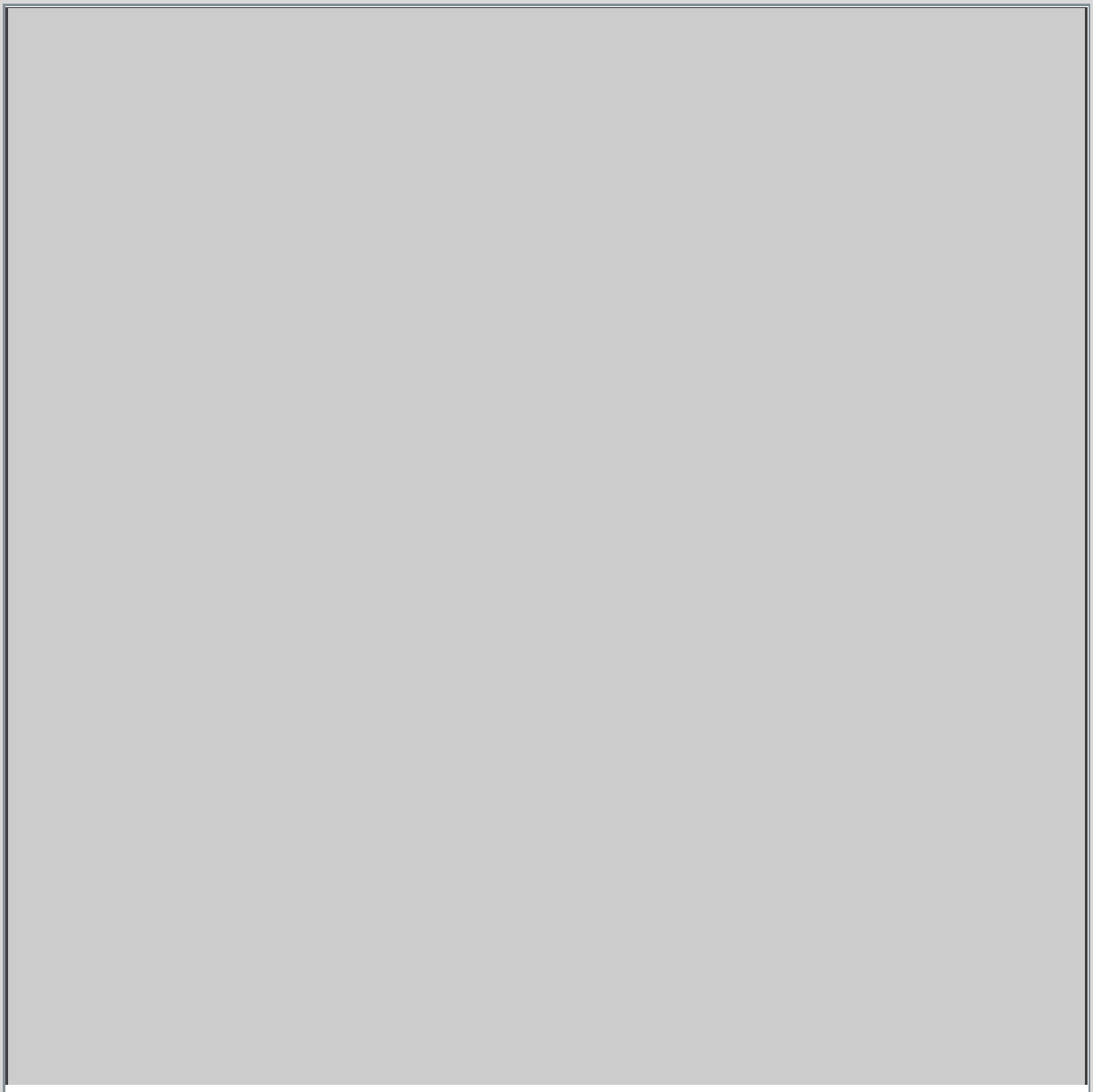
From: NW3C <training@nw3c.org>
To: dominic.boggia@cookcountyil.gov, Dominic Boggia (Sheriff) <Dominic.Boggia@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:06 PM CDT
Received: June 30, 2020 11:10:09 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

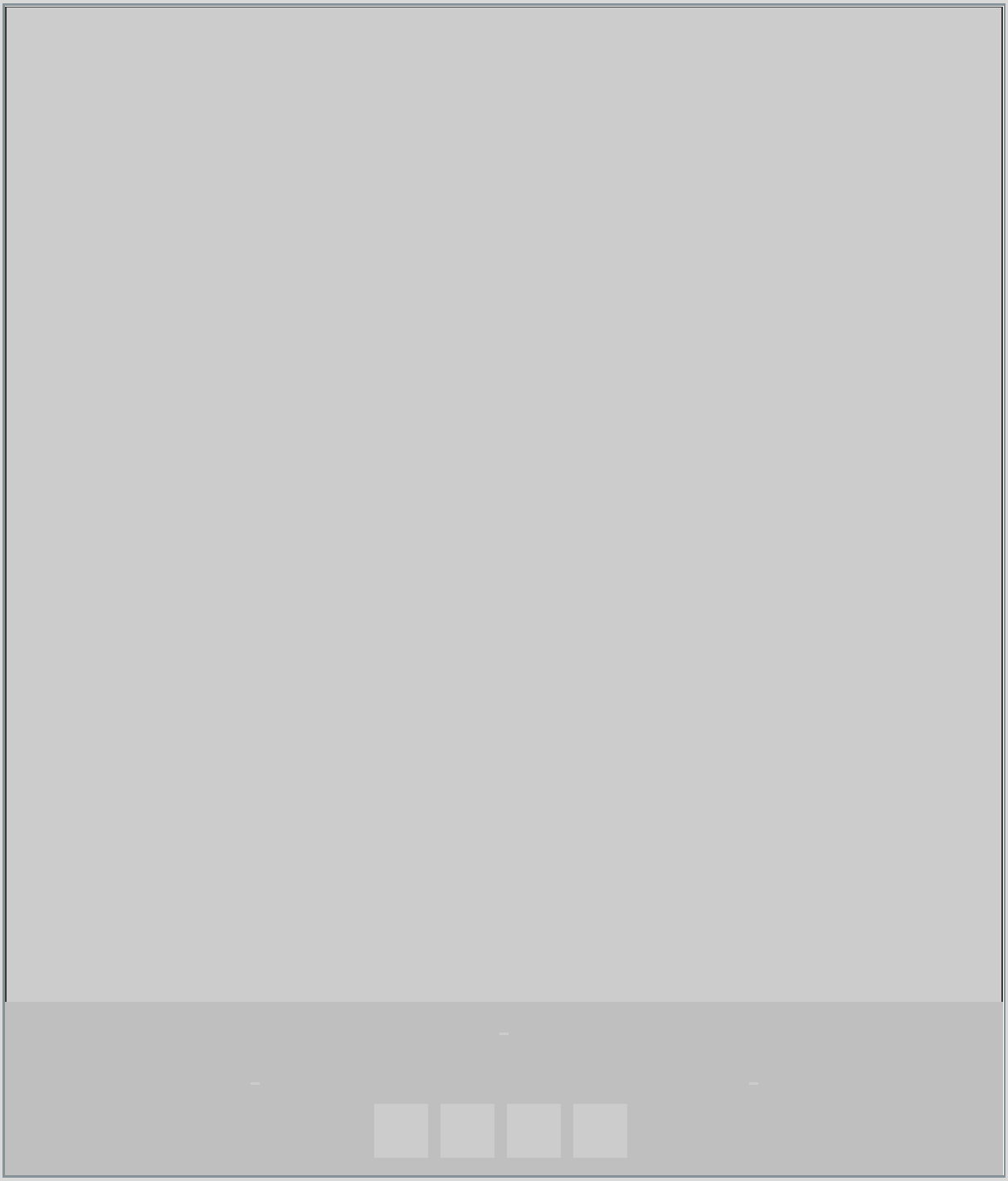
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

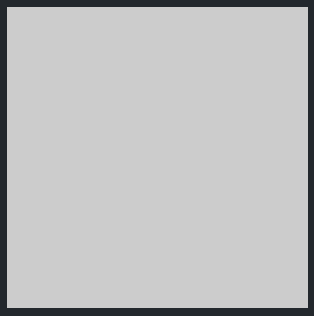
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Dominic Boggia (Sheriff)
Sent:	June 30, 2020 11:10:06 PM CDT
Received:	June 30, 2020 11:10:10 PM CDT

New courses available!

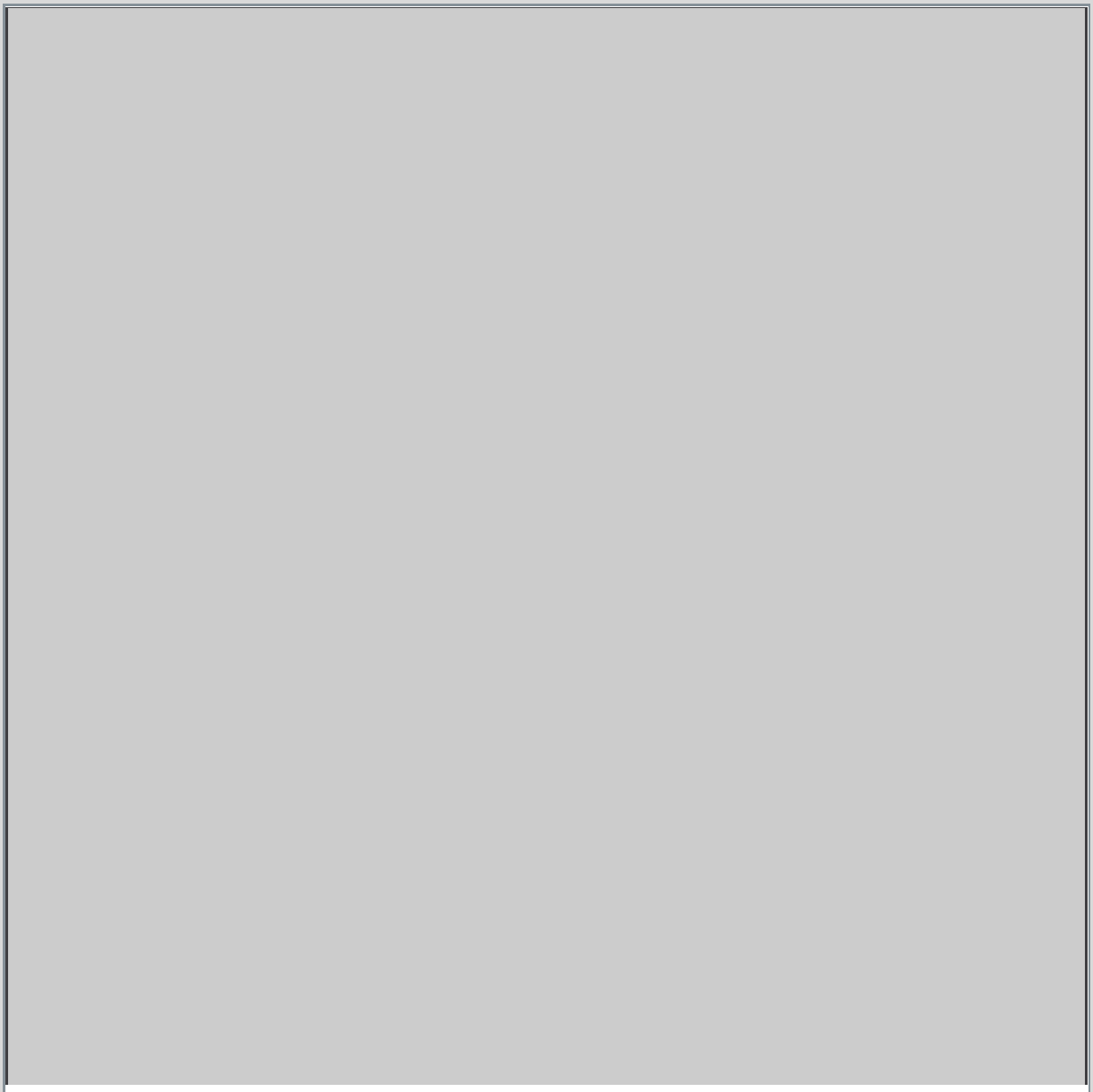
From: NW3C <training@nw3c.org>
To: nicholas.bohlsen@cookcountyil.gov, Nicholas Bohlsen (Sheriff) <Nicholas.Bohlsen@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:07 PM CDT
Received: June 30, 2020 11:10:10 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

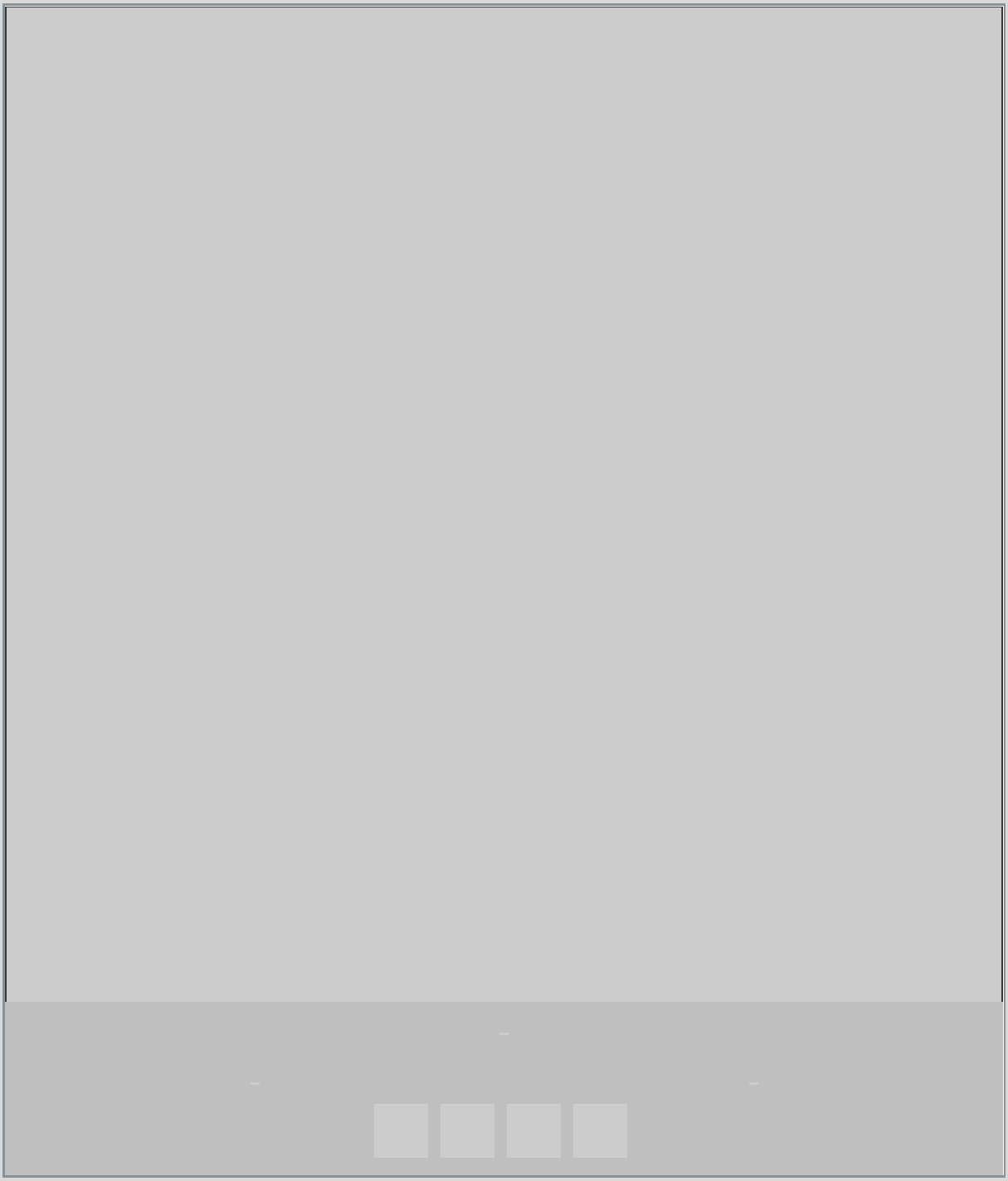
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

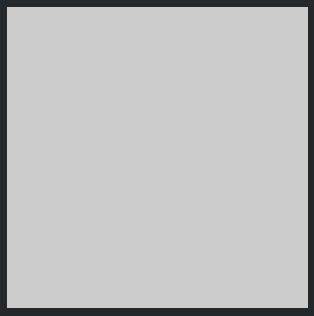
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

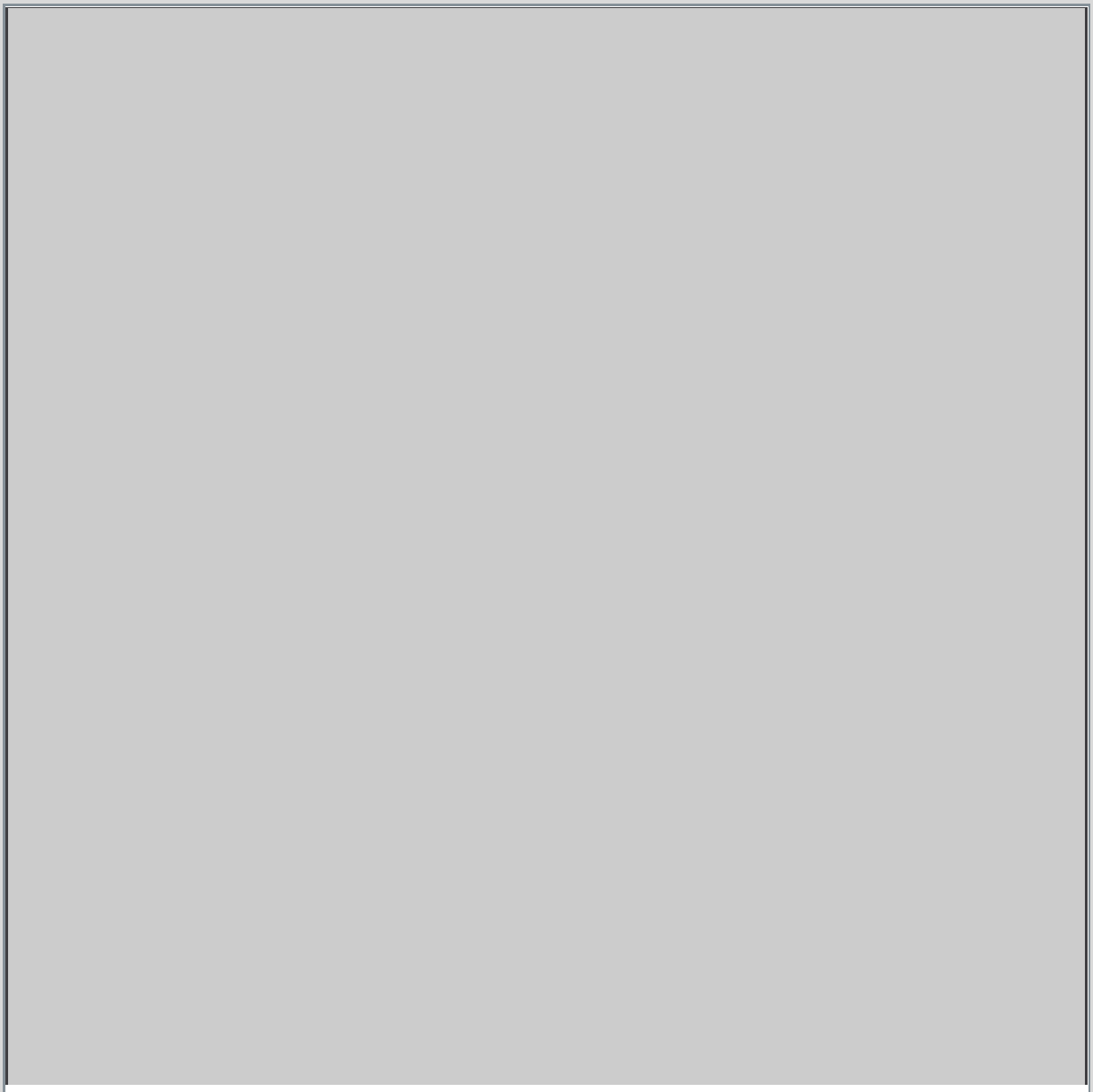
New courses available!

From:	NW3C <training@nw3c.org>
To:	keith.gray@cookcountyil.gov, Keith Gray (Sheriff) <Keith.Gray@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:07 PM CDT
Received:	June 30, 2020 11:10:12 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

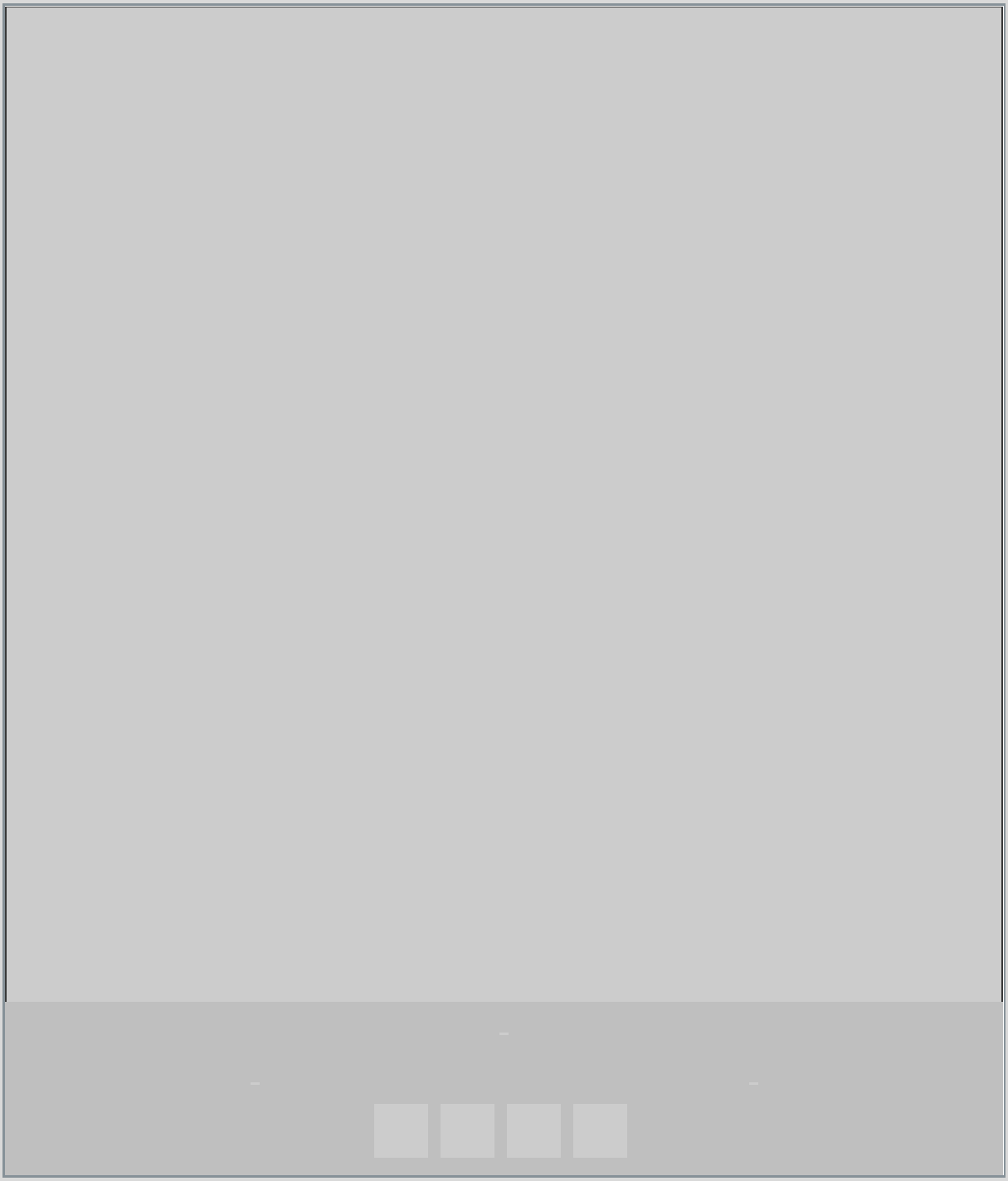
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

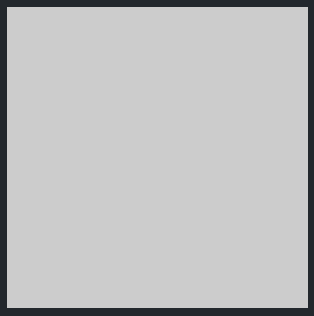
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

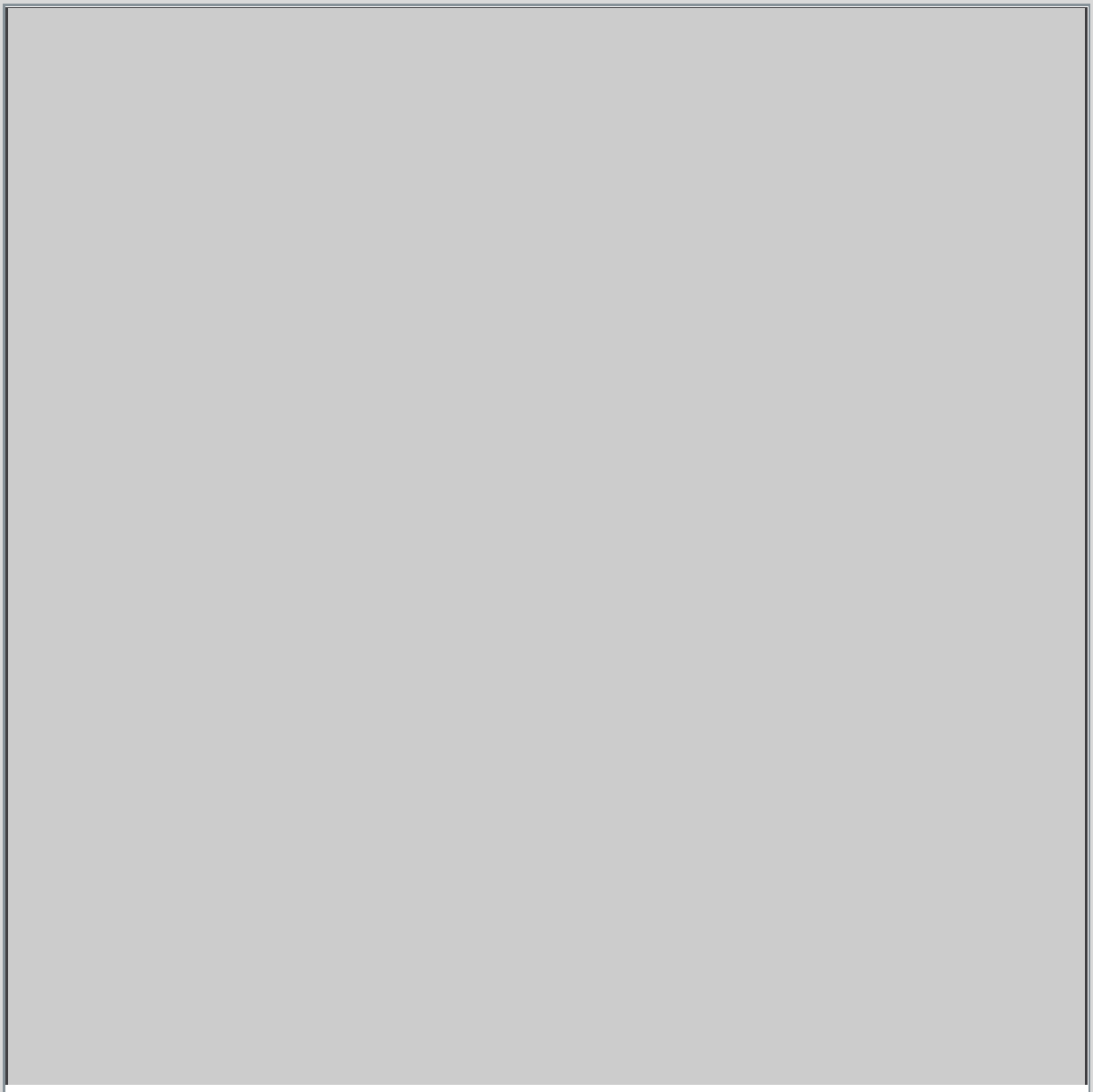
From: NW3C <training@nw3c.org>
To: raymond.struck@cookcountyil.gov, Raymond Struck (Sheriff) <Raymond.Struck@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:07 PM CDT
Received: June 30, 2020 11:10:11 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

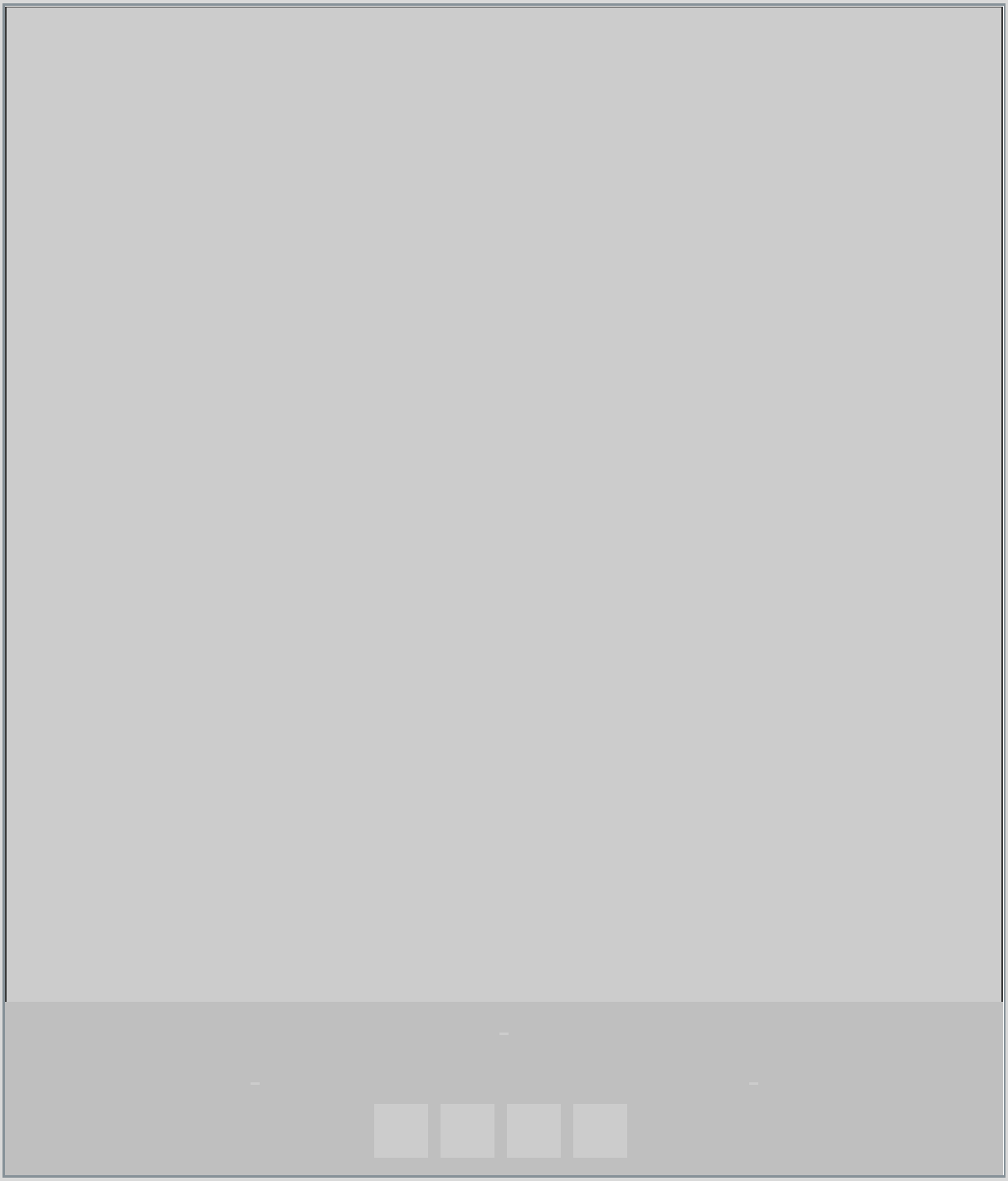
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

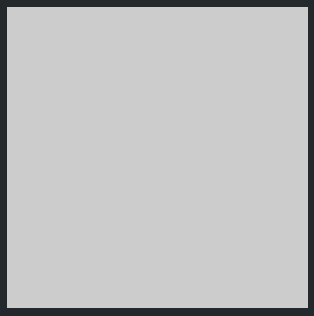
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Nicholas Bohlsen (Sheriff)
Sent:	June 30, 2020 11:10:07 PM CDT
Received:	June 30, 2020 11:10:11 PM CDT

New courses available!

To:	Keith Gray (Sheriff)
Sent:	June 30, 2020 11:10:07 PM CDT
Received:	June 30, 2020 11:10:12 PM CDT

New courses available!

To:	Raymond Struck (Sheriff)
Sent:	June 30, 2020 11:10:07 PM CDT
Received:	June 30, 2020 11:10:12 PM CDT

New courses available!

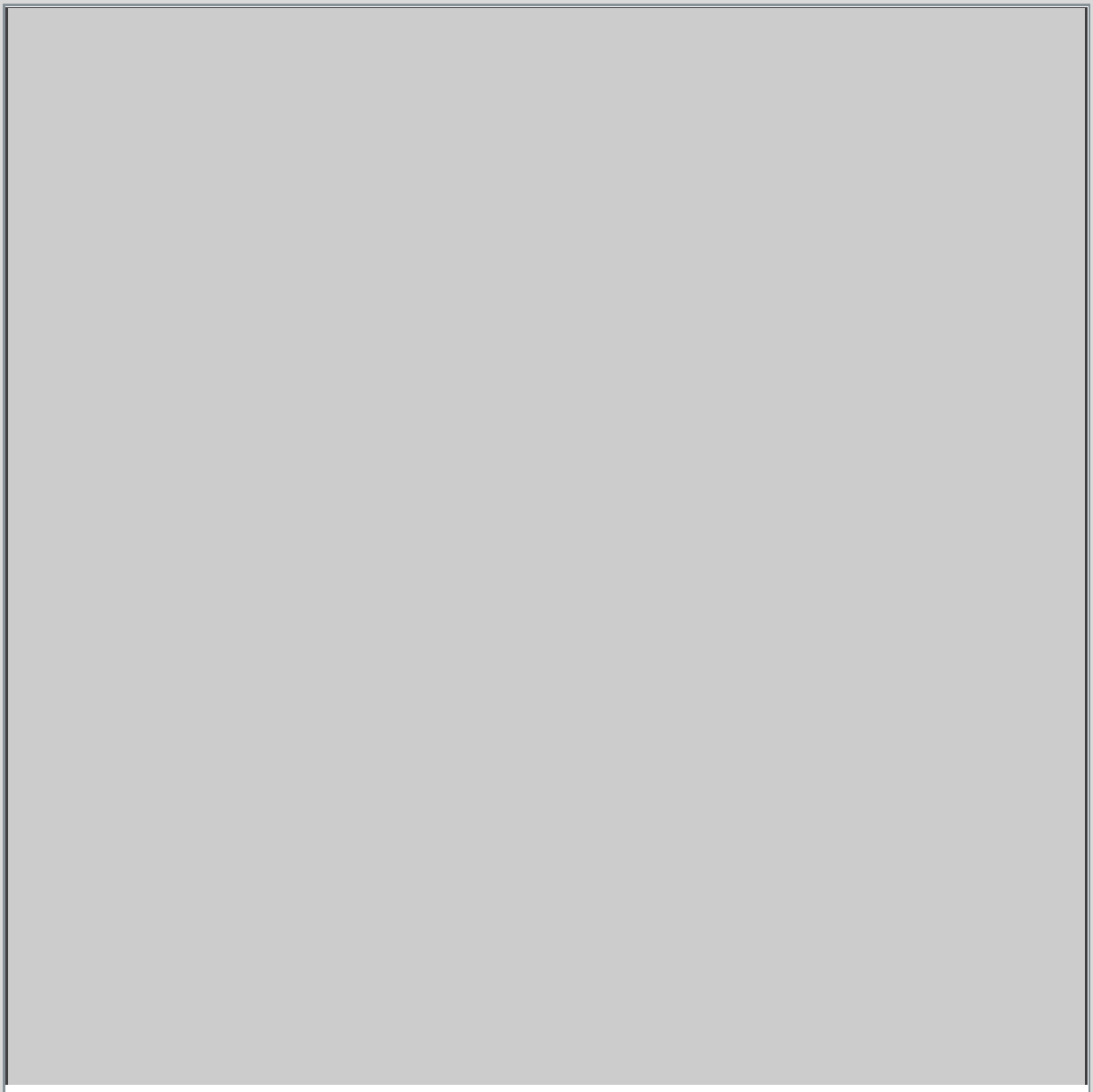
From: NW3C <training@nw3c.org>
To: robert.lobacz@cookcountyil.gov, Robert Lobacz (Sheriff) <Robert.Lobacz@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:08 PM CDT
Received: June 30, 2020 11:10:11 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

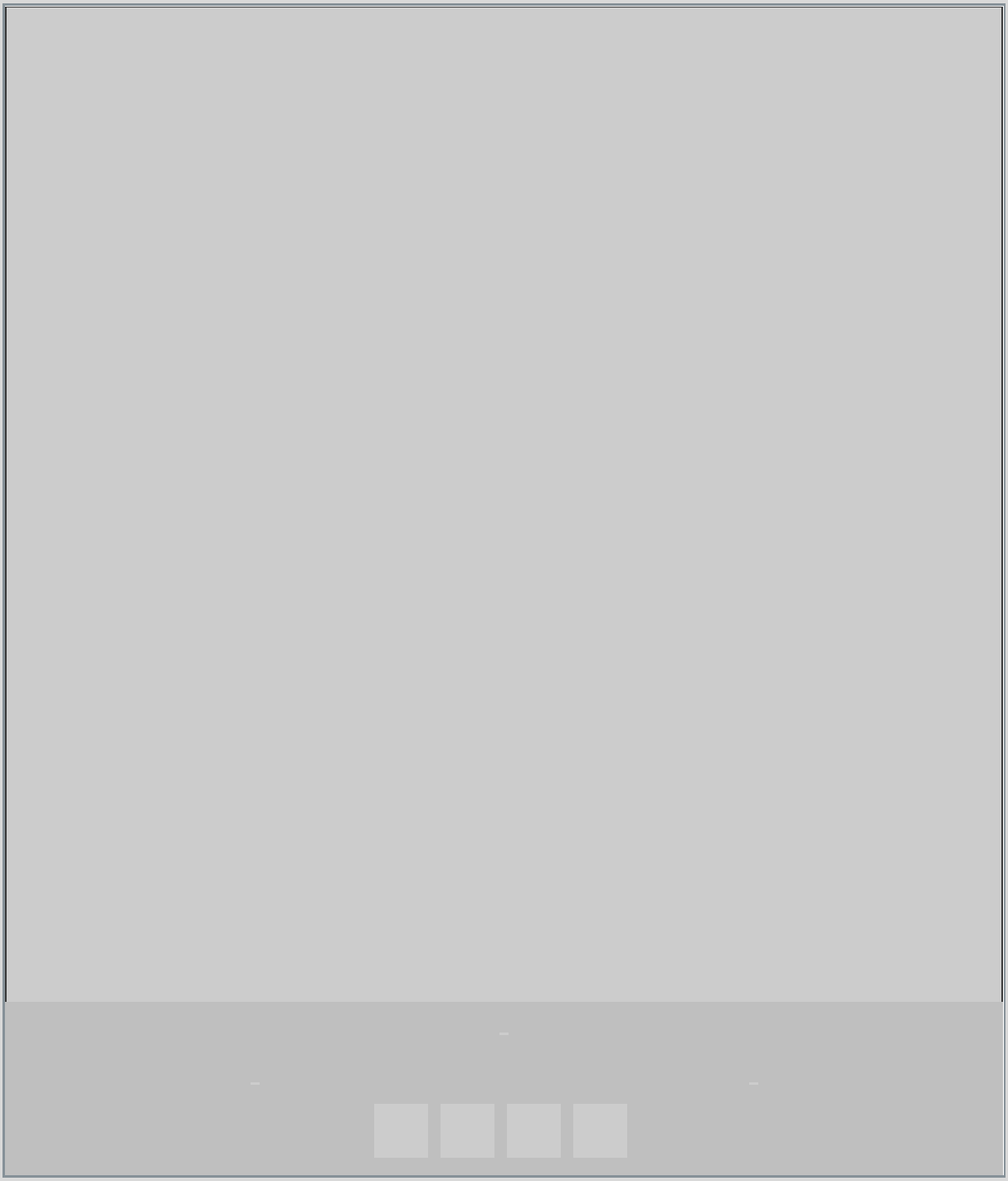
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

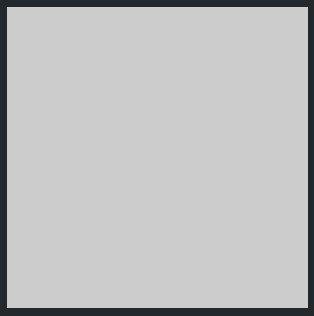
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

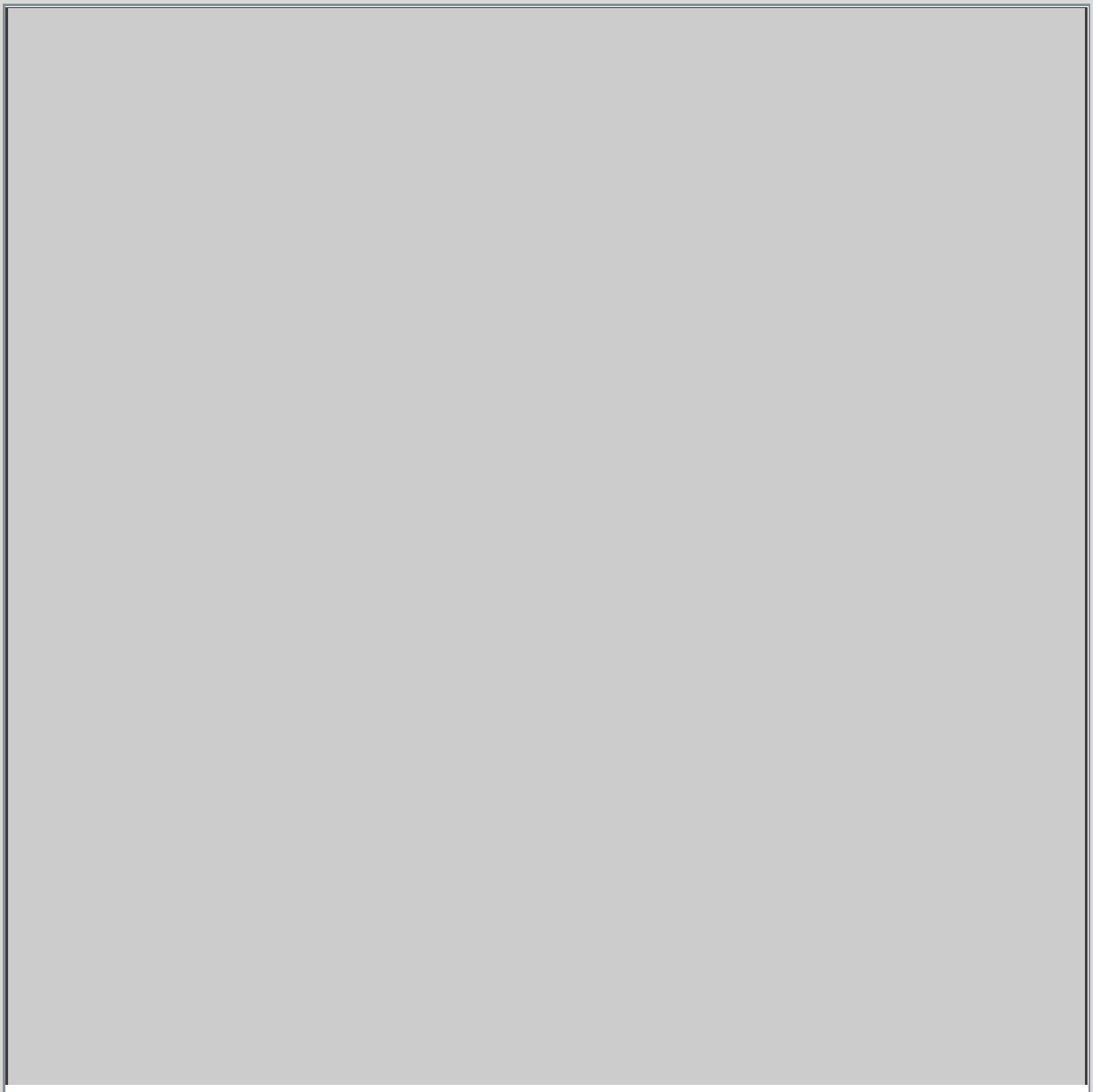
New courses available!

From:	NW3C <training@nw3c.org>
To:	jonathan.janulis@cookcountyil.gov, Jonathan Janulis (Sheriff) <Jonathan.Janulis@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:08 PM CDT
Received:	June 30, 2020 11:10:13 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

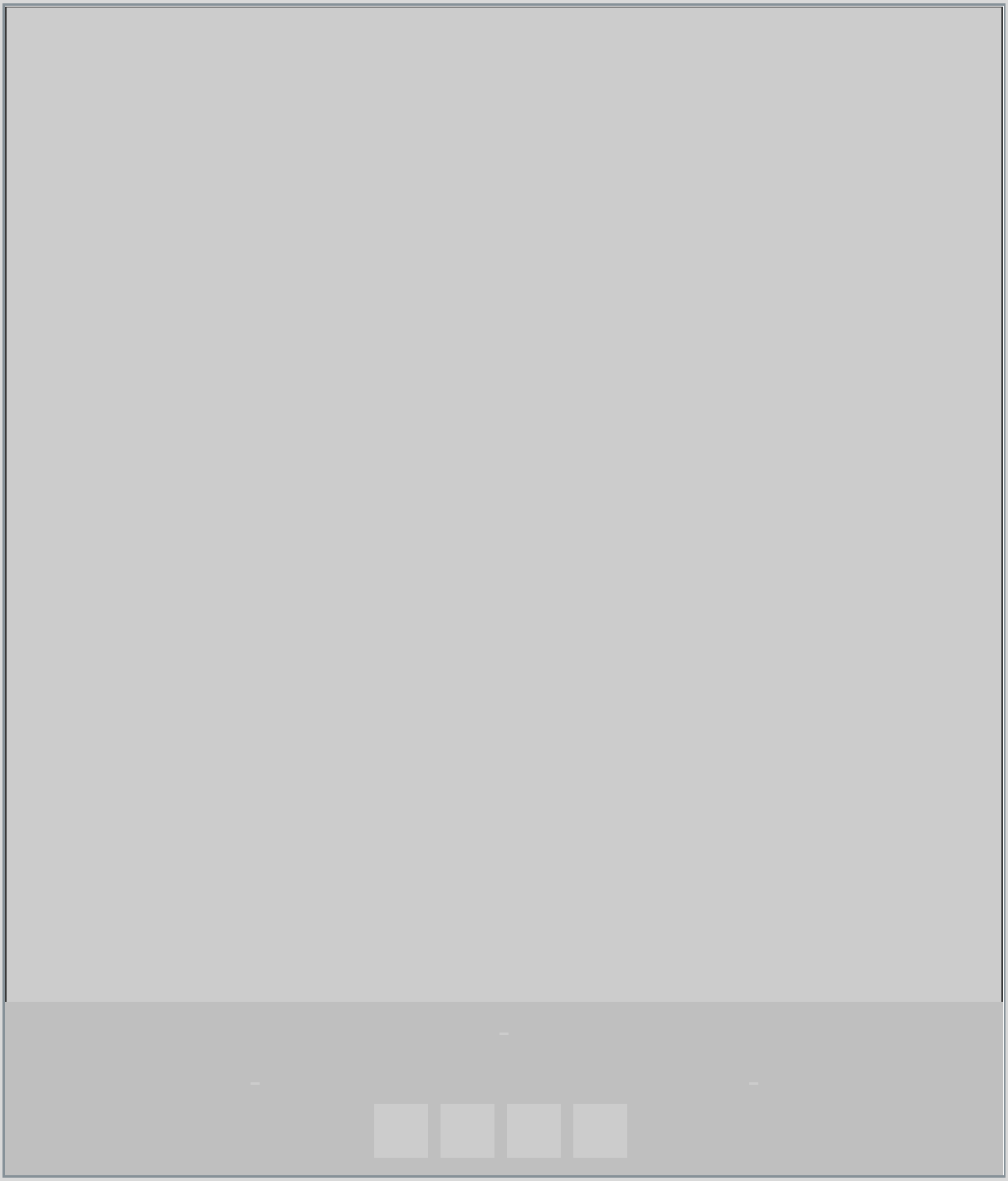
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

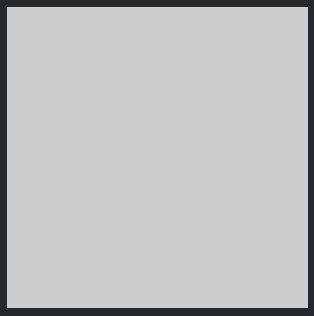
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

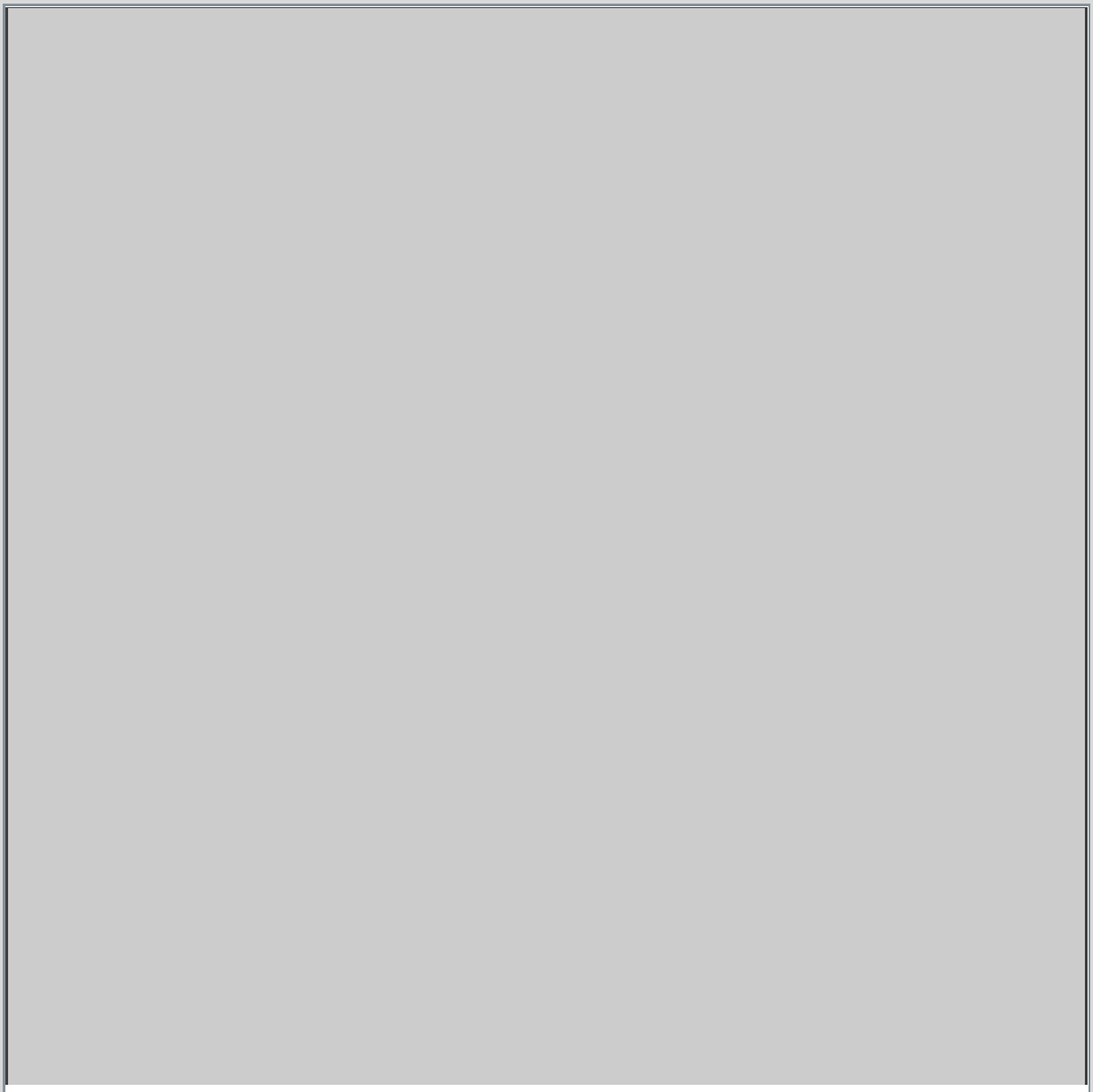
New courses available!

From:	NW3C <training@nw3c.org>
To:	robert.ruminski@cookcountyil.gov, Robert Ruminski (Sheriff) <Robert.Ruminski@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:08 PM CDT
Received:	June 30, 2020 11:10:11 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

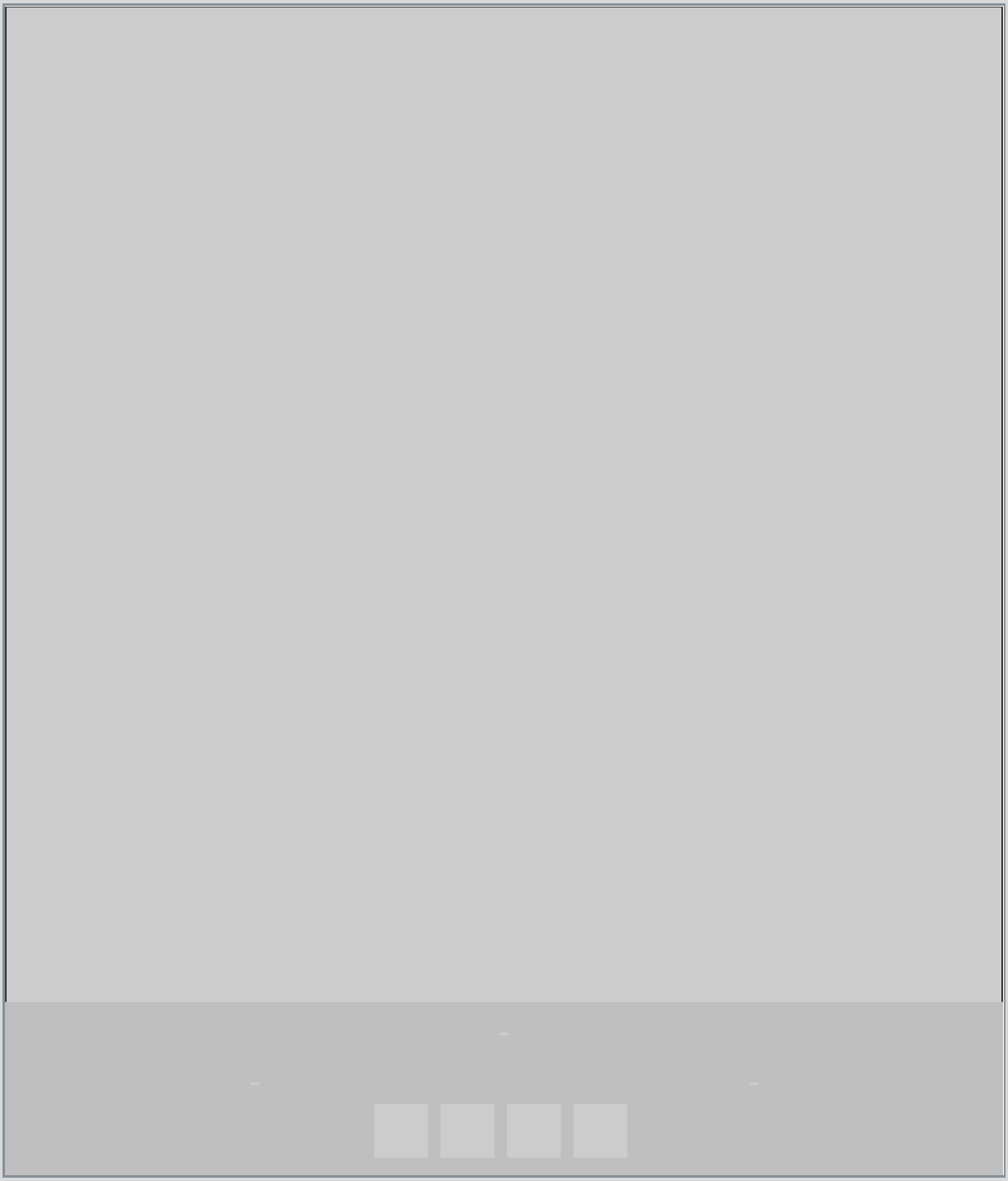
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

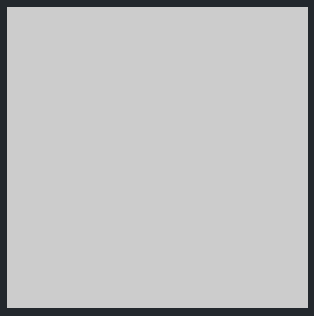
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Robert Lobacz (Sheriff)
Sent:	June 30, 2020 11:10:08 PM CDT
Received:	June 30, 2020 11:10:12 PM CDT

New courses available!

To:	Jonathan Janulis (Sheriff)
Sent:	June 30, 2020 11:10:08 PM CDT
Received:	June 30, 2020 11:10:14 PM CDT

New courses available!

To:	Robert Ruminski (Sheriff)
Sent:	June 30, 2020 11:10:08 PM CDT
Received:	June 30, 2020 11:10:12 PM CDT

New courses available!

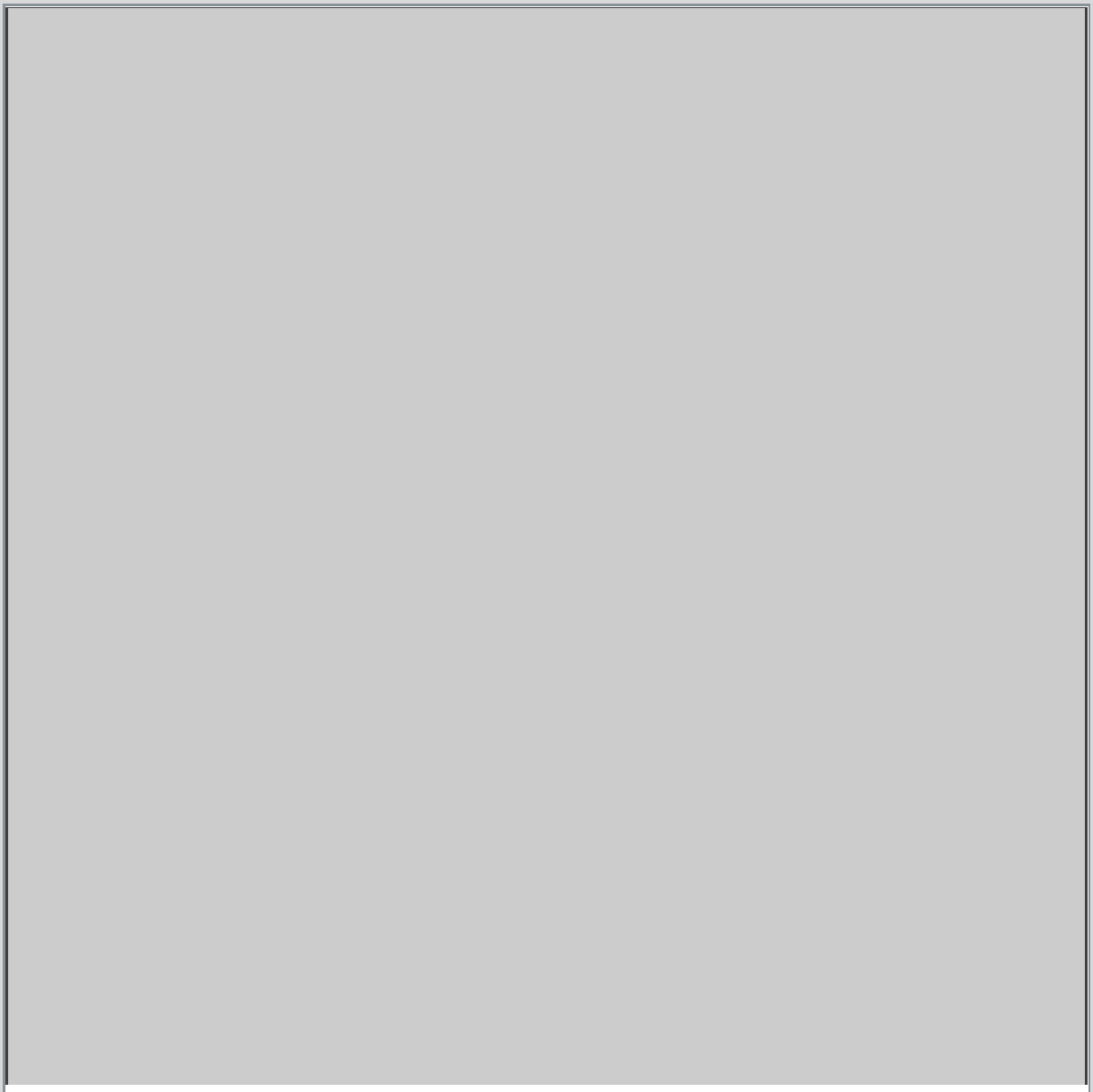
From: NW3C <training@nw3c.org>
To: jimeal.haddad@cookcountyil.gov, Jimeal Haddad (Sheriff) <Jimeal.Haddad@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:09 PM CDT
Received: June 30, 2020 11:10:11 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

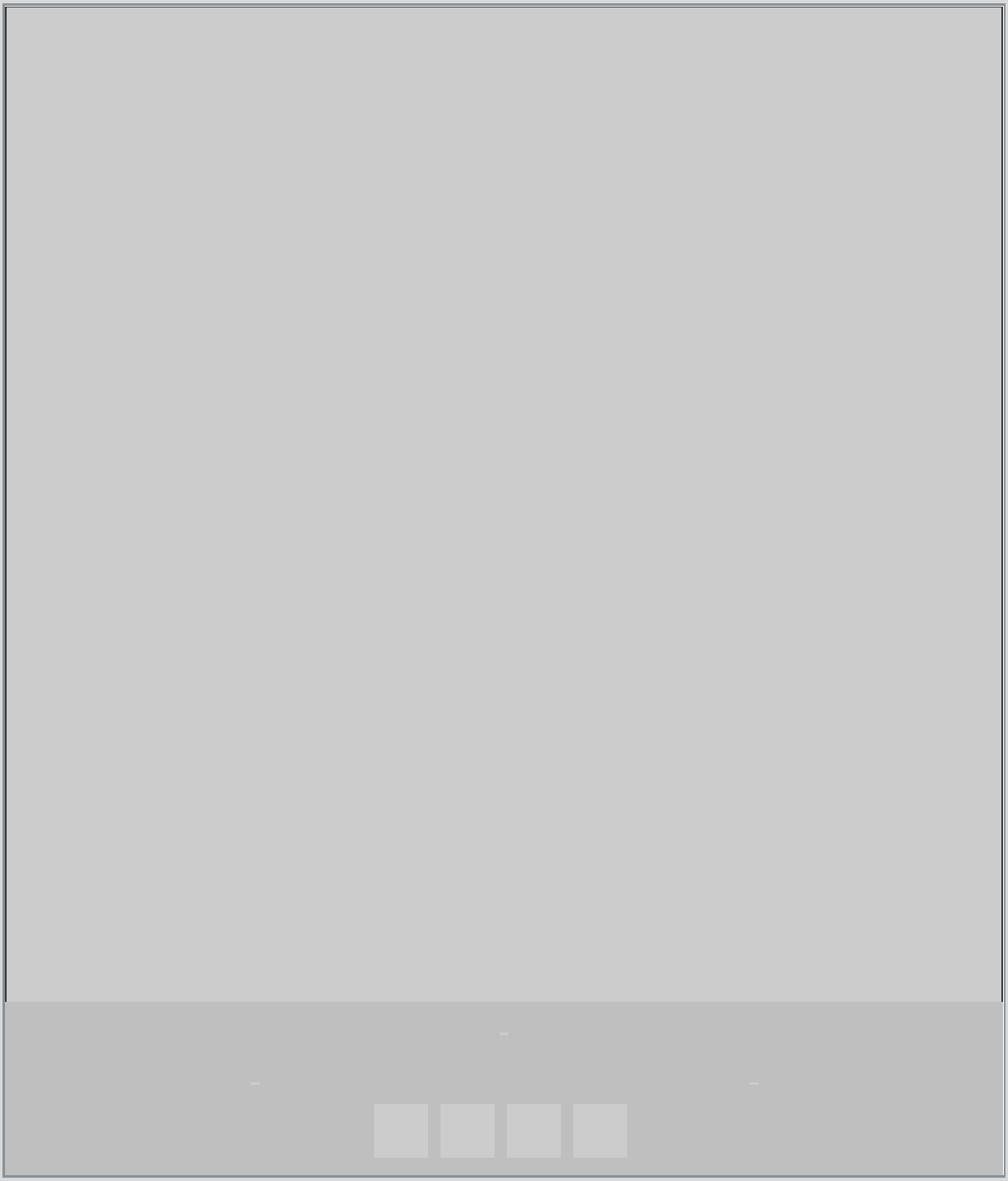
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

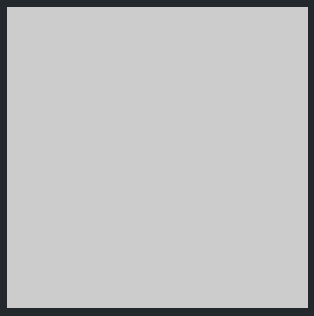
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

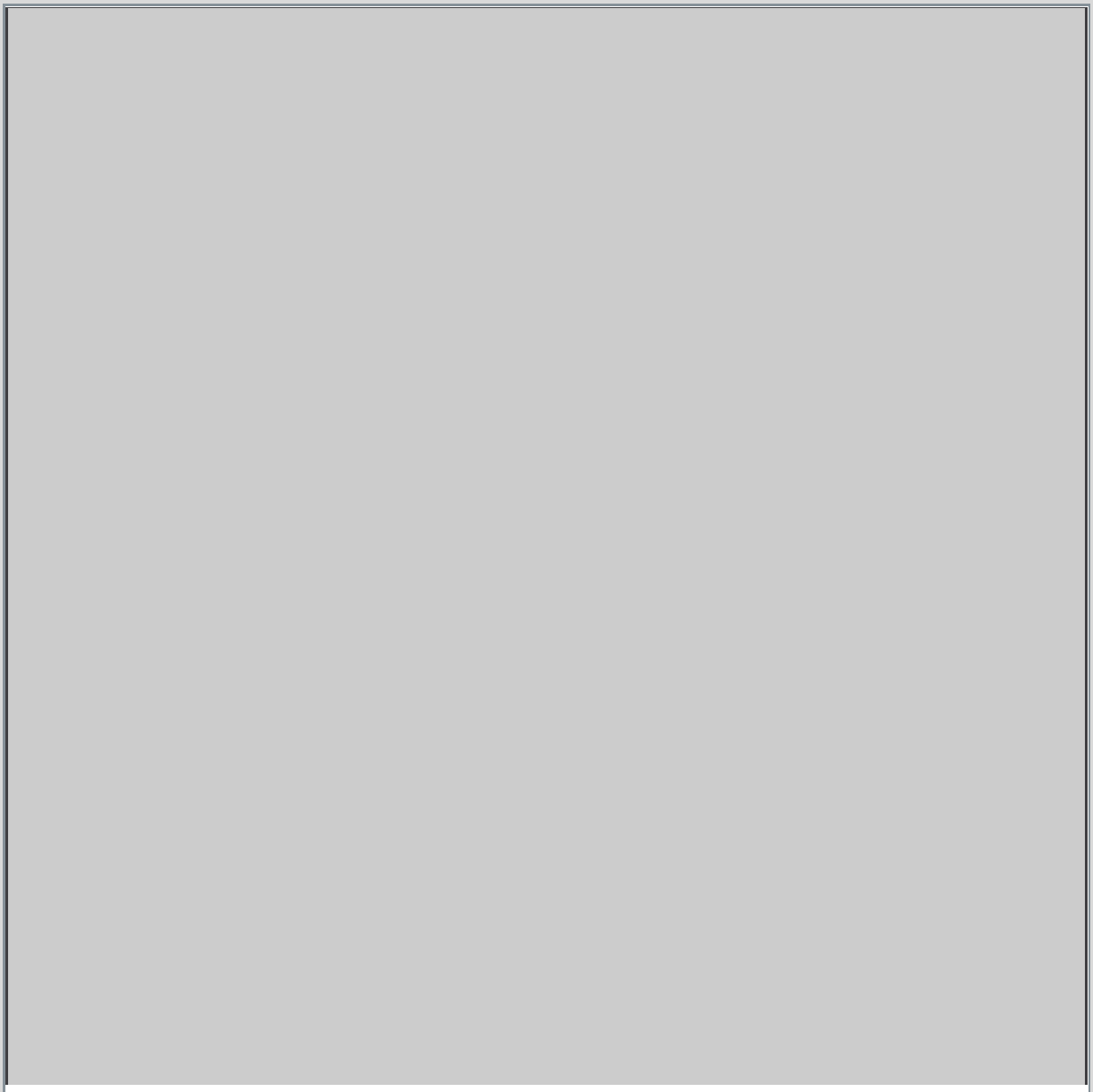
From: NW3C <training@nw3c.org>
To: elliott.reyes@cookcountyil.gov, Elliott Reyes (Sheriff) <Elliott.Reyes@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:09 PM CDT
Received: June 30, 2020 11:10:16 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

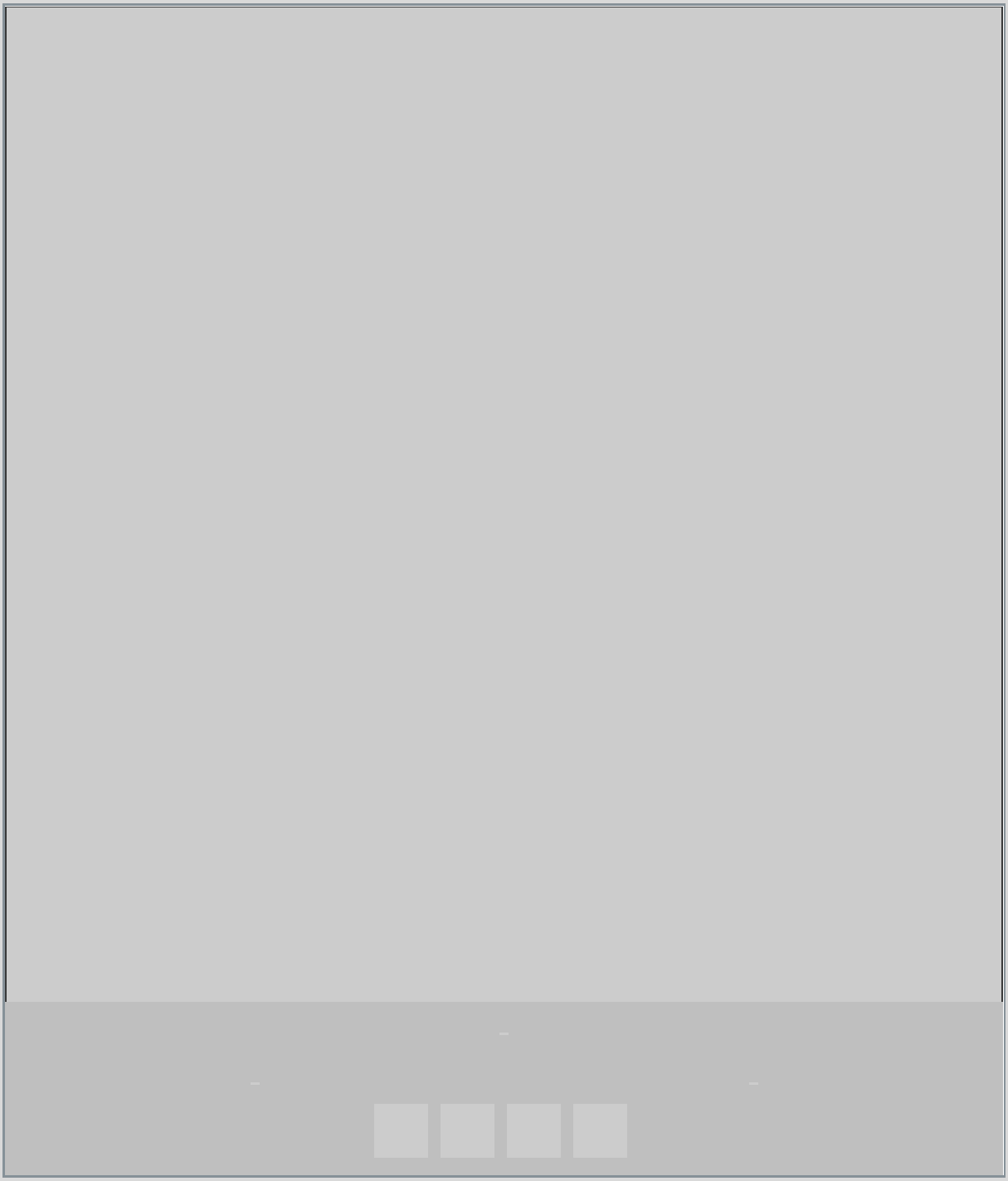
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

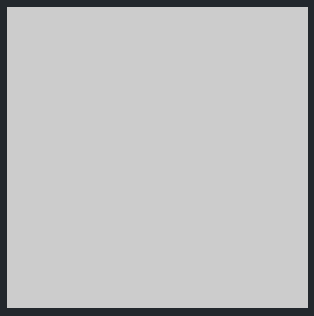
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

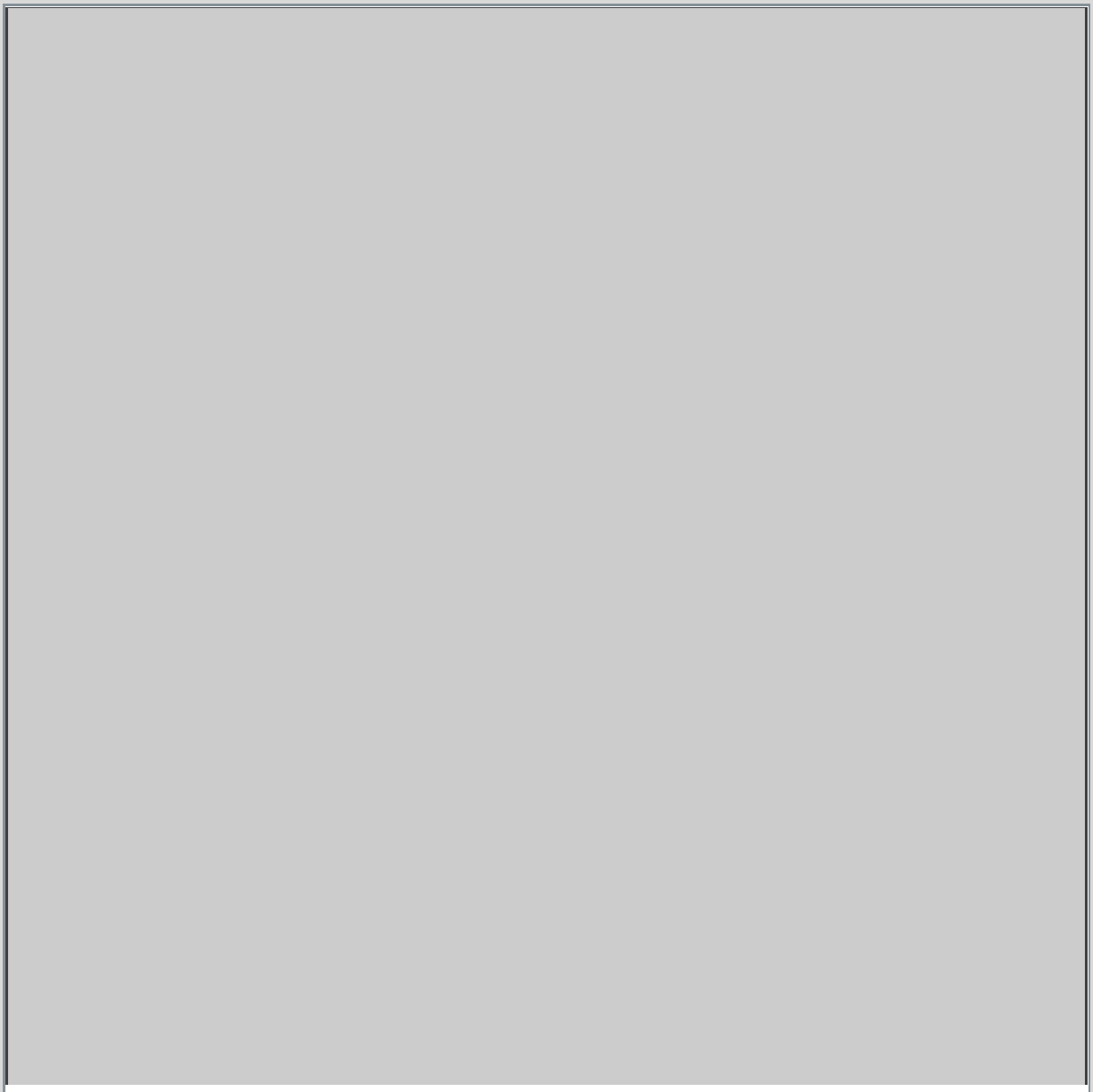
New courses available!

From:	NW3C <training@nw3c.org>
To:	katherine.walsh@cookcountyil.gov, Katherine Walsh (Sheriff) <Katherine.Walsh@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:09 PM CDT
Received:	June 30, 2020 11:10:17 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

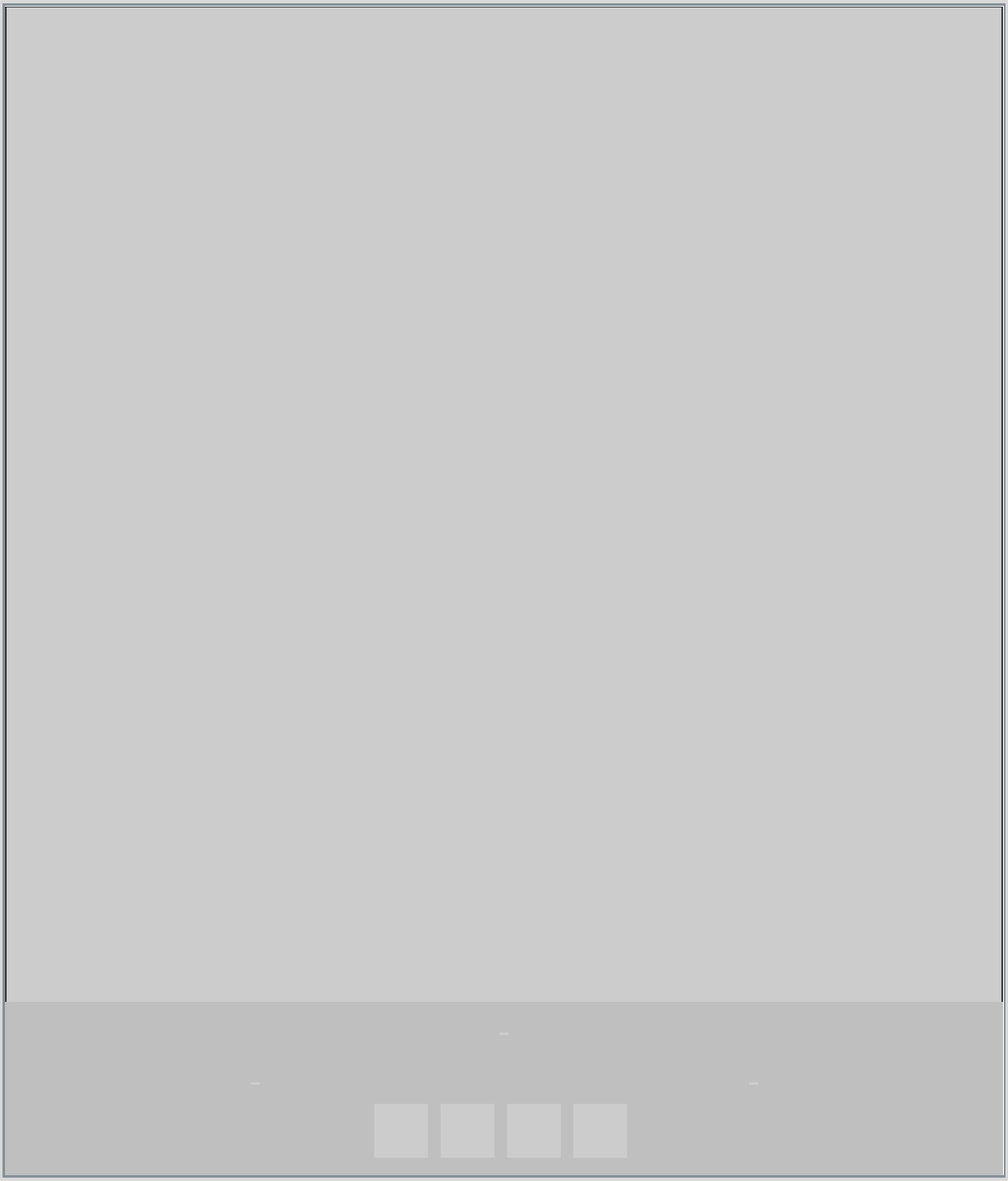
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

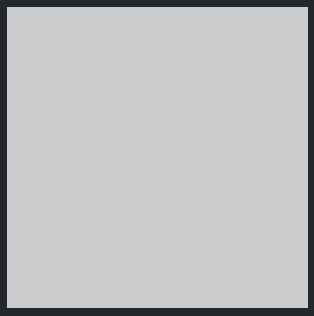
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

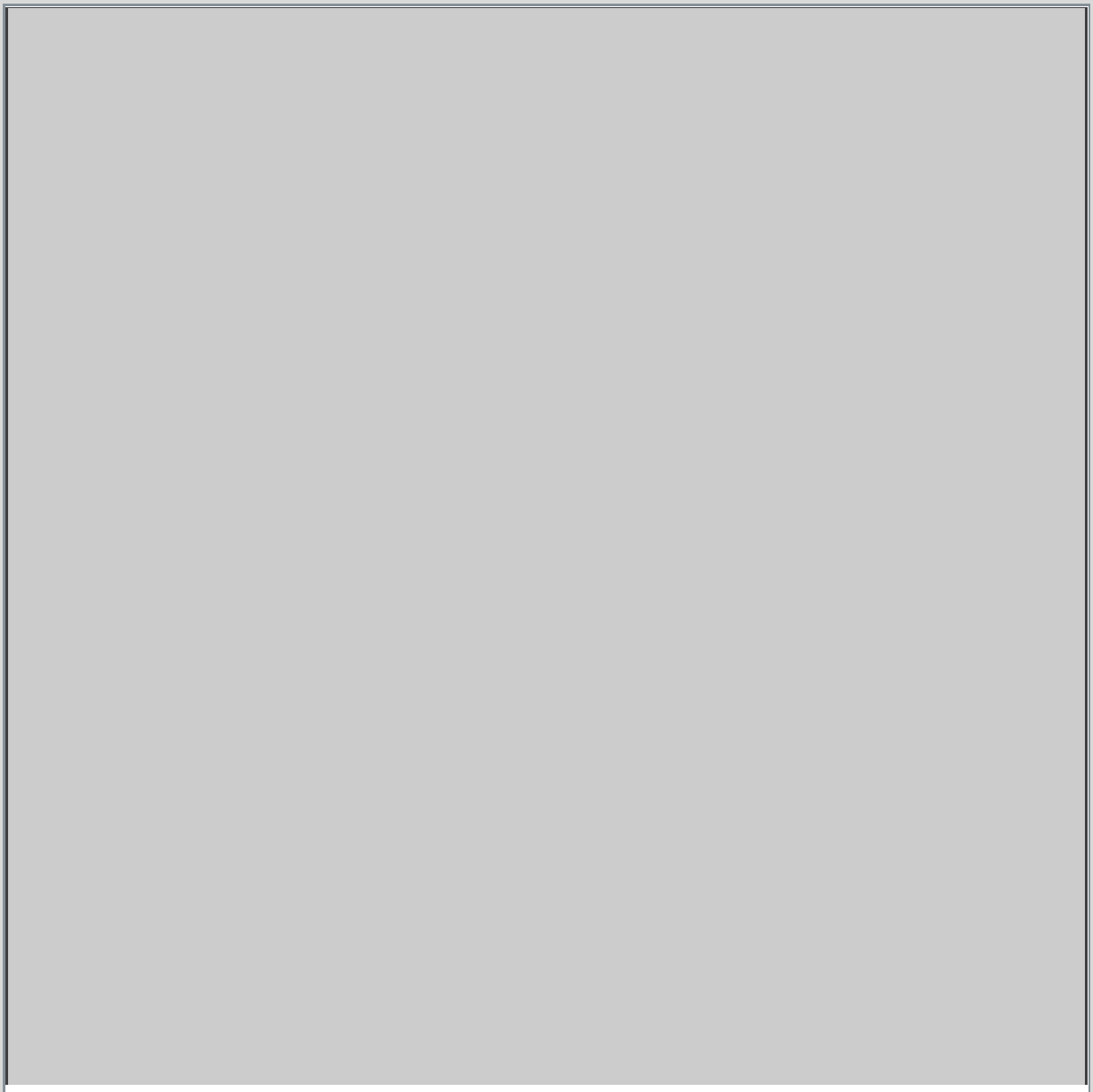
From: NW3C <training@nw3c.org>
To: patrick.donovan@cookcountyil.gov, Patrick Donovan (Sheriff) <Patrick.Donovan@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:09 PM CDT
Received: June 30, 2020 11:10:15 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

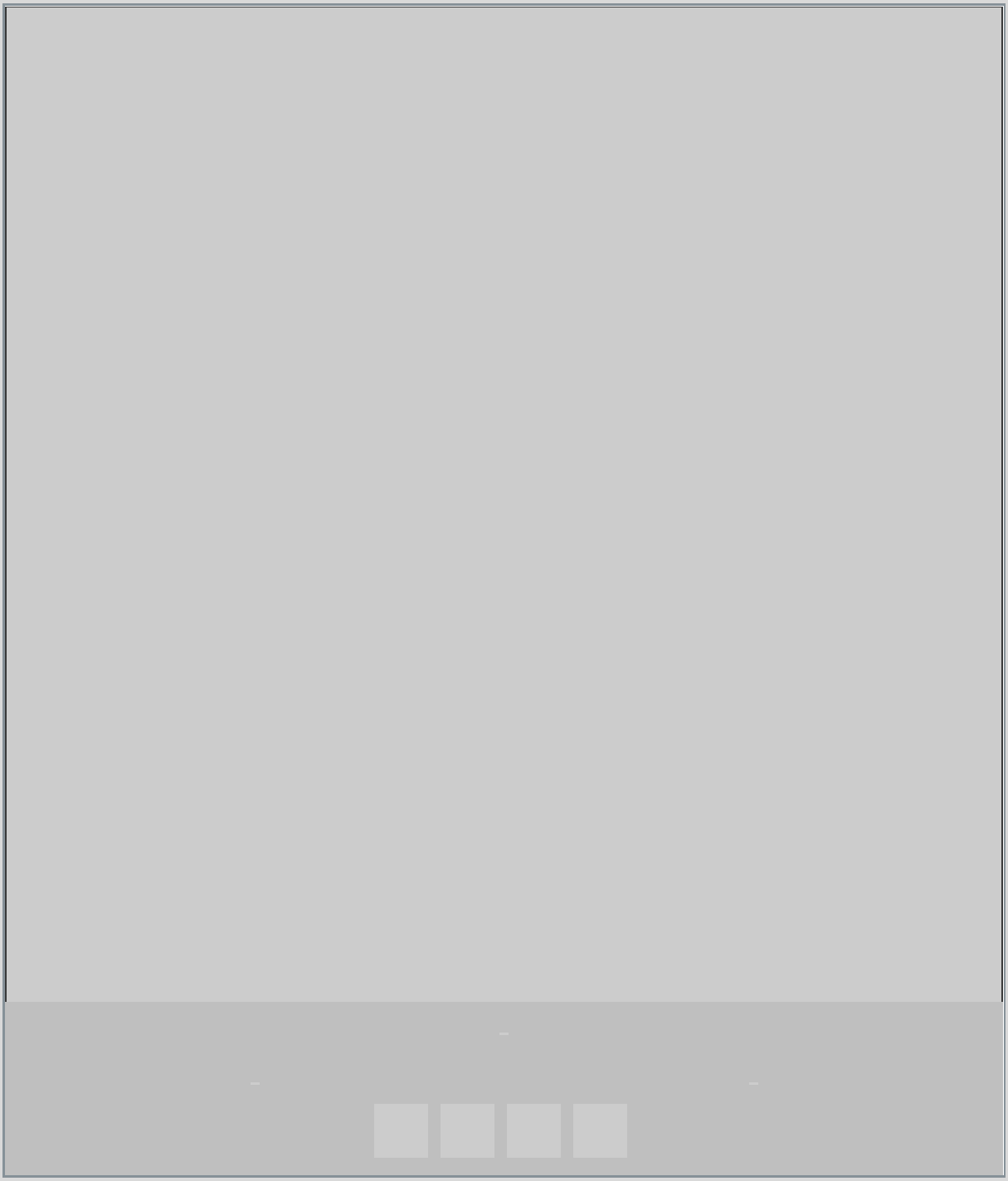
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

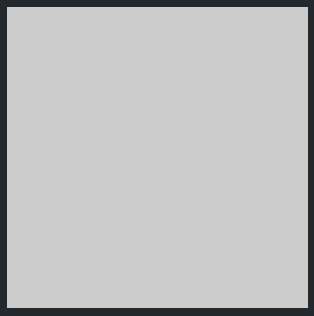
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Jimeal Haddad (Sheriff)
Sent:	June 30, 2020 11:10:09 PM CDT
Received:	June 30, 2020 11:10:12 PM CDT

New courses available!

To:	Elliott Reyes (Sheriff)
Sent:	June 30, 2020 11:10:09 PM CDT
Received:	June 30, 2020 11:10:17 PM CDT

New courses available!

To:	Katherine Walsh (Sheriff)
Sent:	June 30, 2020 11:10:09 PM CDT
Received:	June 30, 2020 11:10:18 PM CDT

New courses available!

To:	Patrick Donovan (Sheriff)
Sent:	June 30, 2020 11:10:09 PM CDT
Received:	June 30, 2020 11:10:15 PM CDT

New courses available!

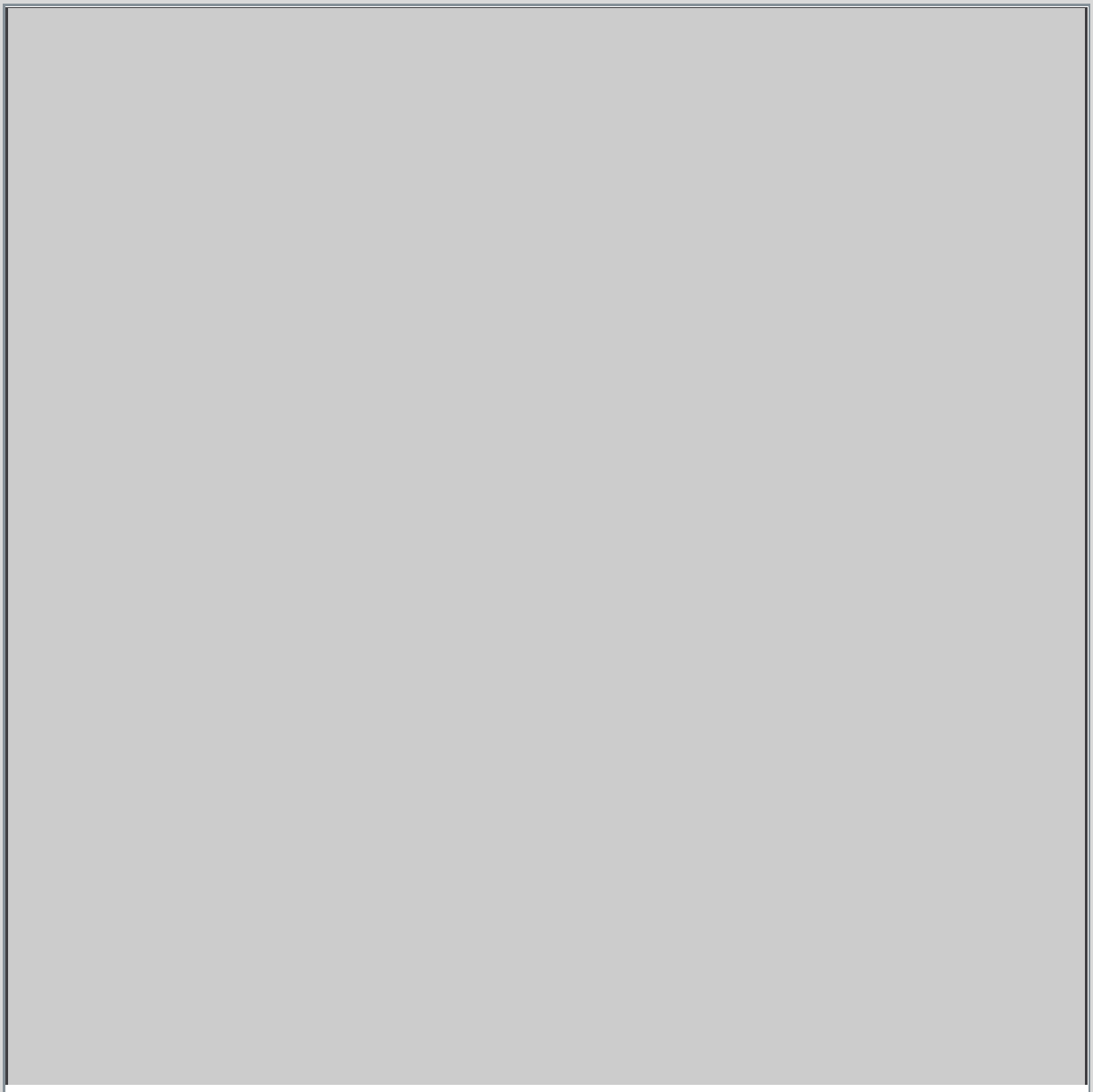
From: NW3C <training@nw3c.org>
To: sean.gleason@cookcountyil.gov, Sean Gleason (Sheriff) <Sean.Gleason@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:10 PM CDT
Received: June 30, 2020 11:10:19 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

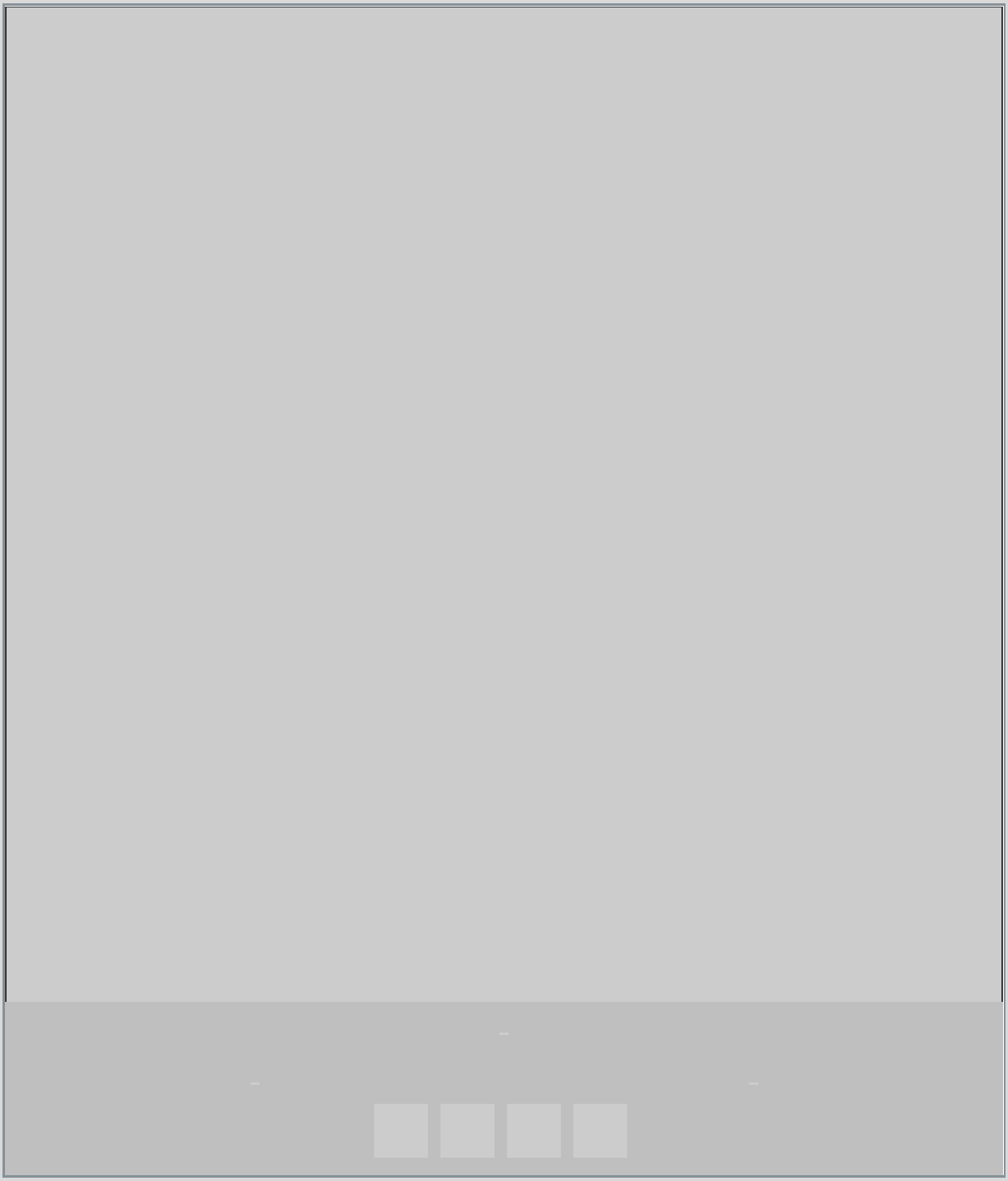
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

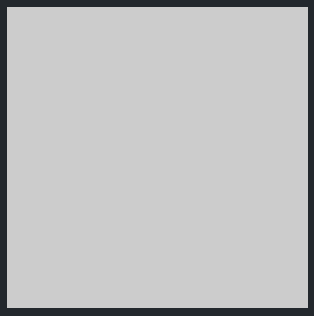
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

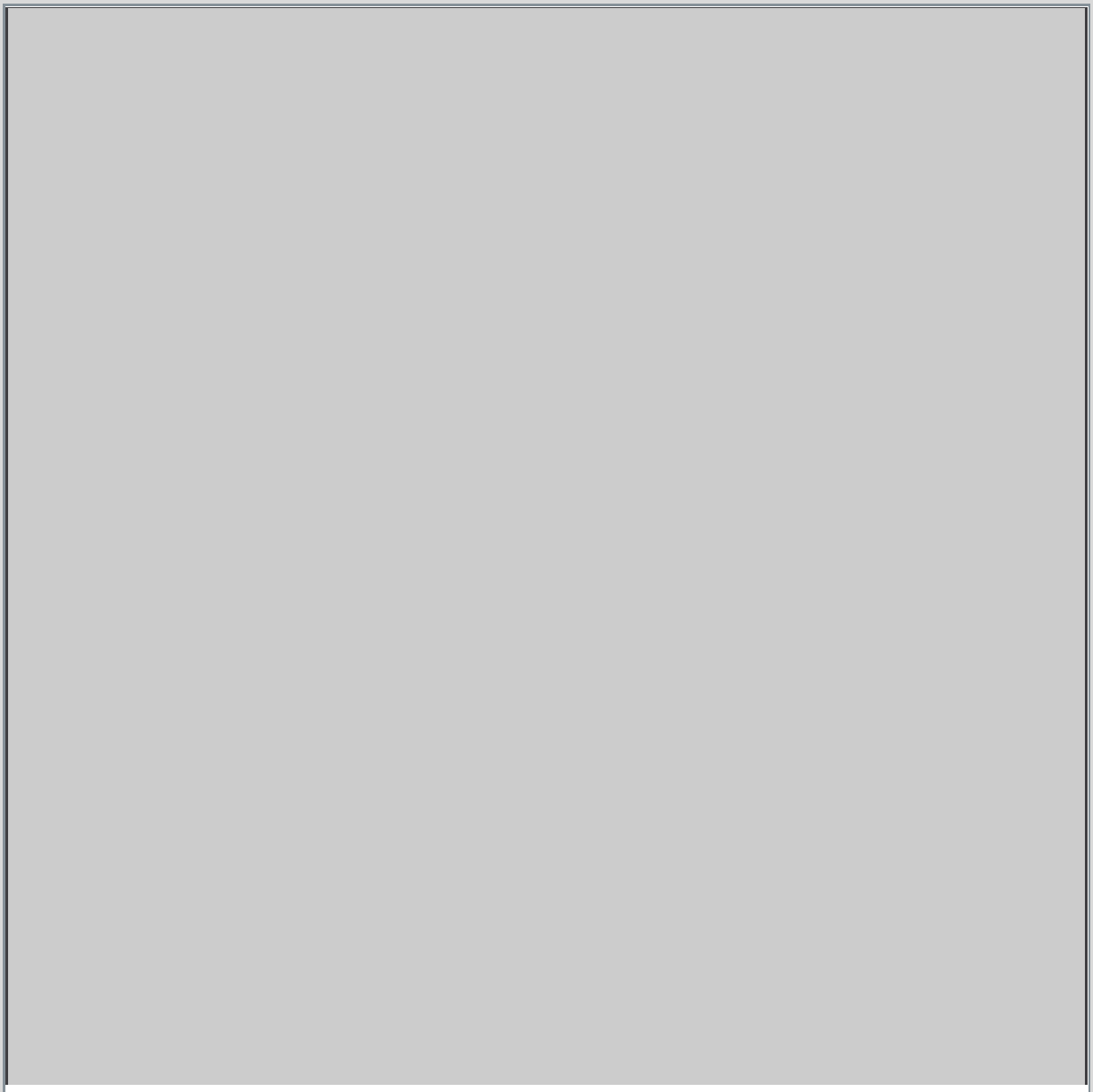
From: NW3C <training@nw3c.org>
To: fontella.brownmarshall@cookcountyil.gov, Fontella BrownMarshall (Sheriff) <fontella.brownmarshall@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:11 PM CDT
Received: June 30, 2020 11:10:13 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

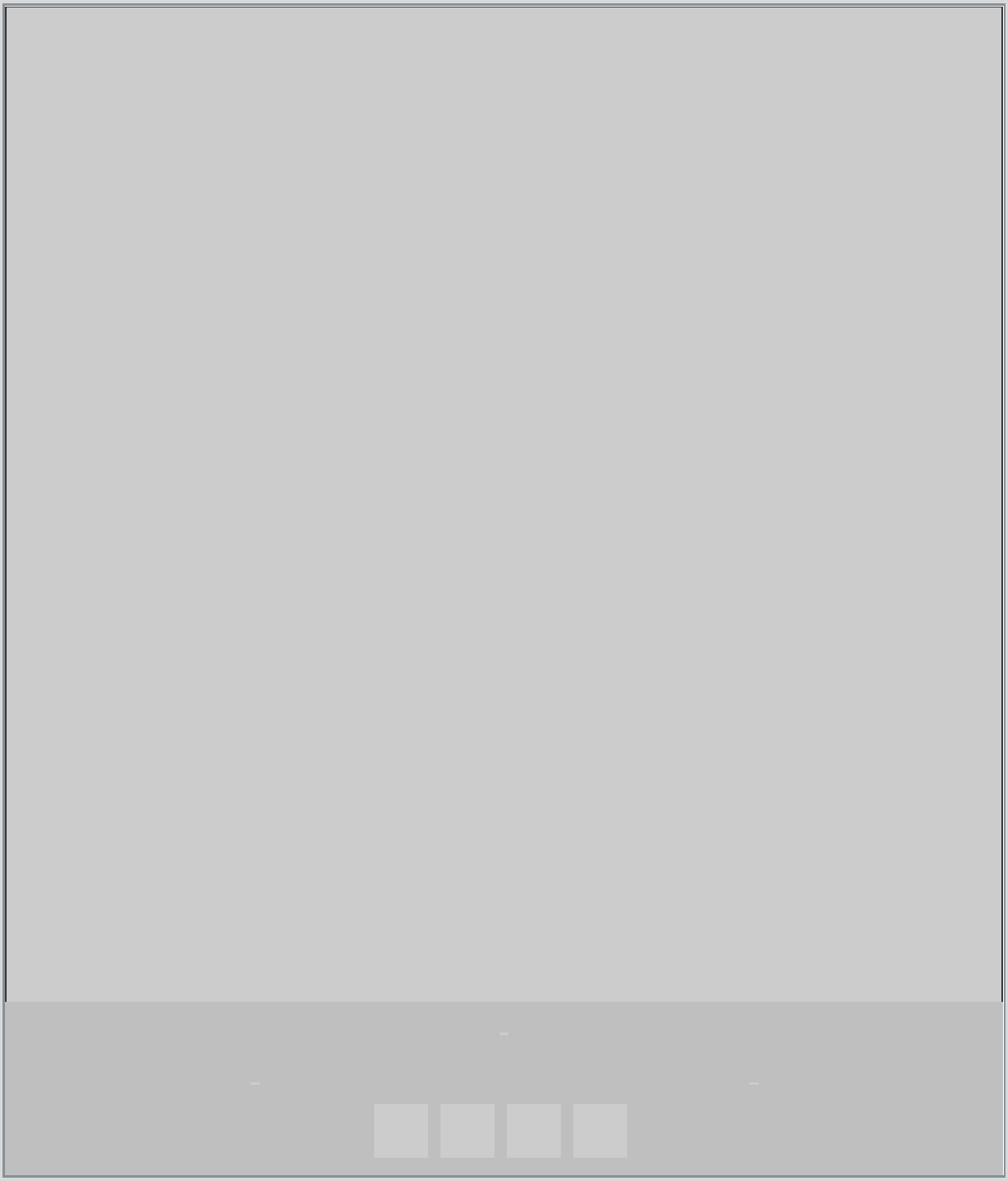
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

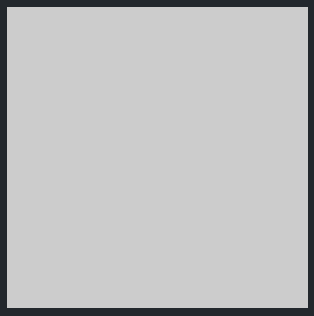
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Fontella BrownMarshall (Sheriff)
Sent:	June 30, 2020 11:10:11 PM CDT
Received:	June 30, 2020 11:10:14 PM CDT

New courses available!

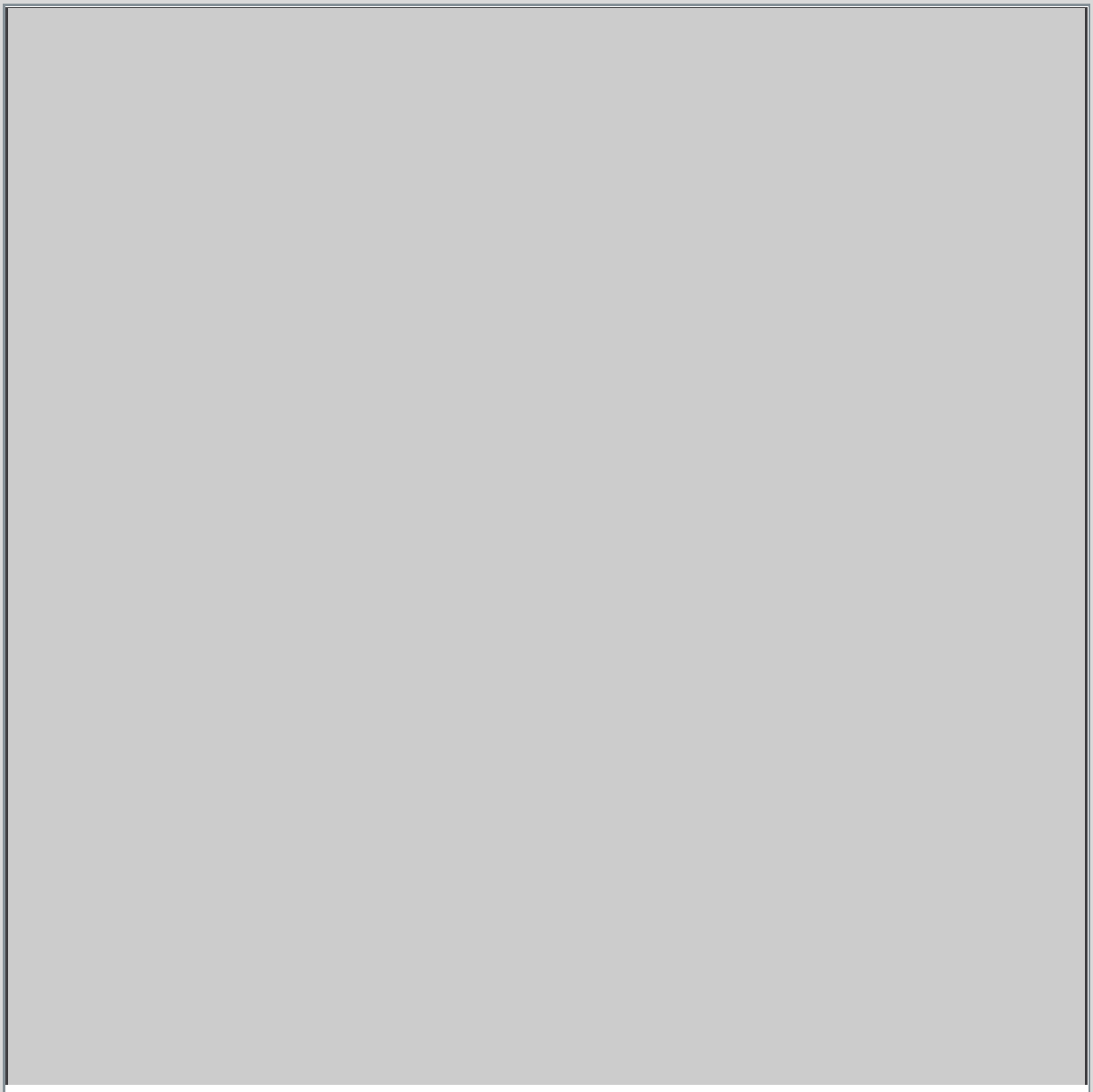
From: NW3C <training@nw3c.org>
To: daniel.redican@cookcountyil.gov, Daniel Redican (Sheriff) <Daniel.Redican@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:14 PM CDT
Received: June 30, 2020 11:10:18 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

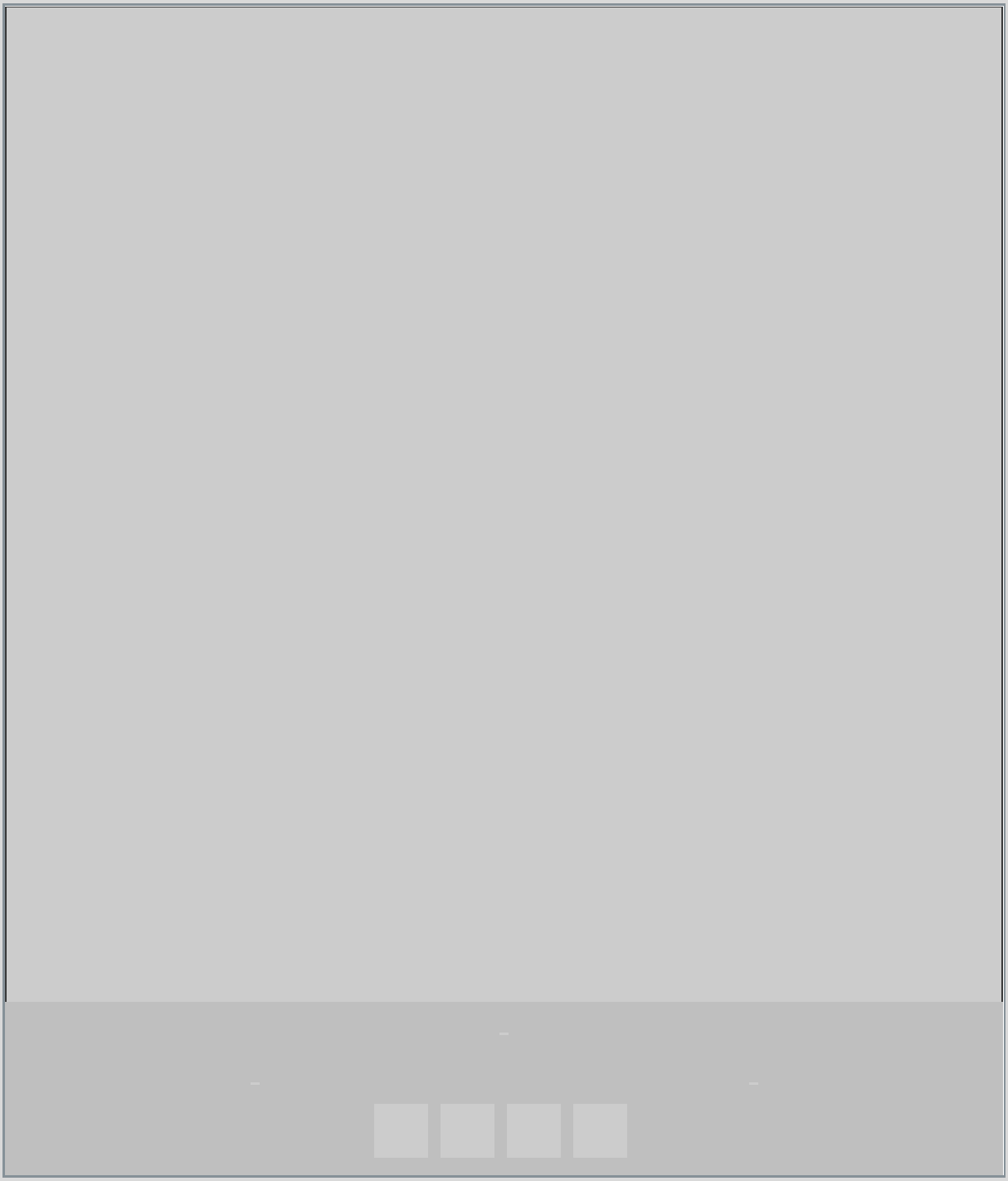
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

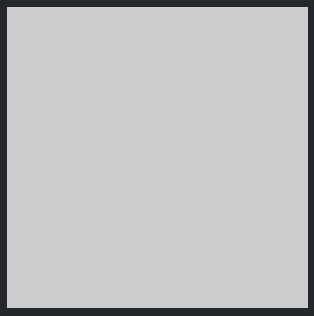
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

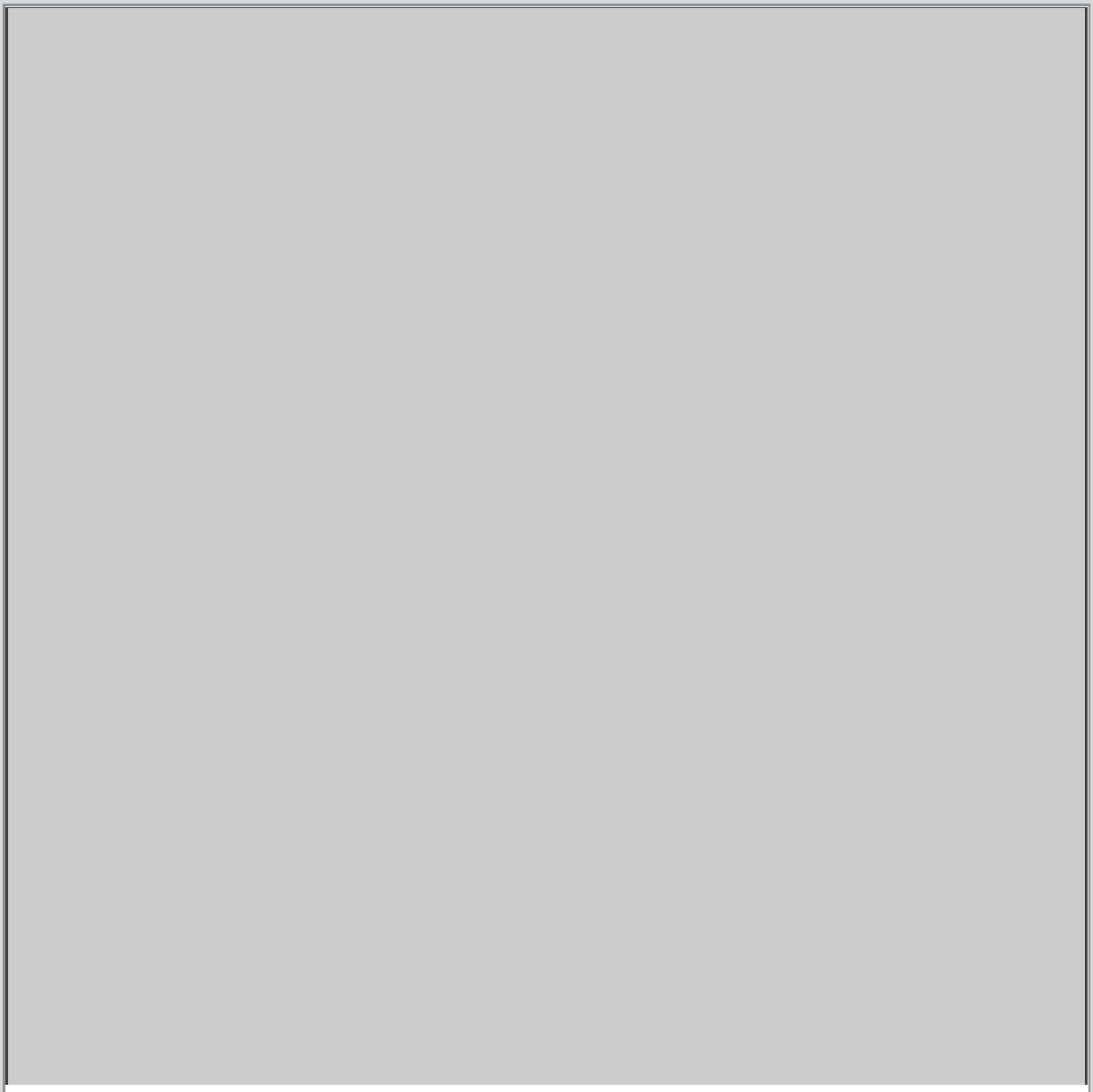
New courses available!

From:	NW3C <training@nw3c.org>
To:	pascal.waller@cookcountyil.gov, Pascal Waller (Sheriff) <Pascal.Waller@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:14 PM CDT
Received:	June 30, 2020 11:10:18 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

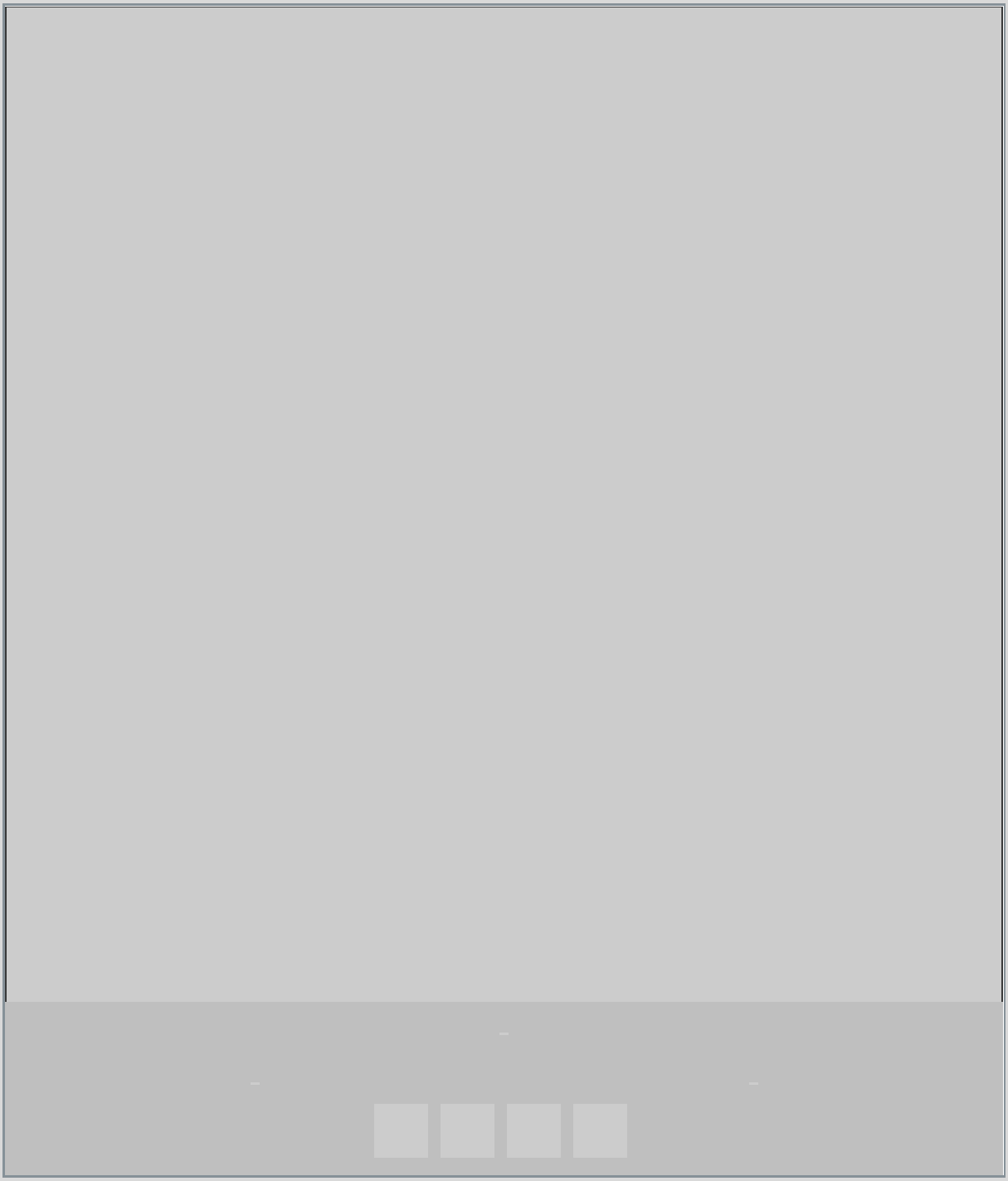
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

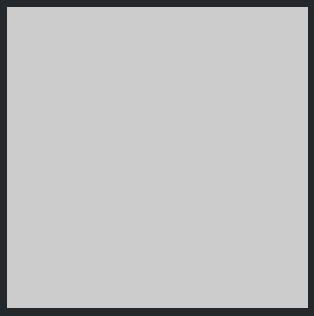
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

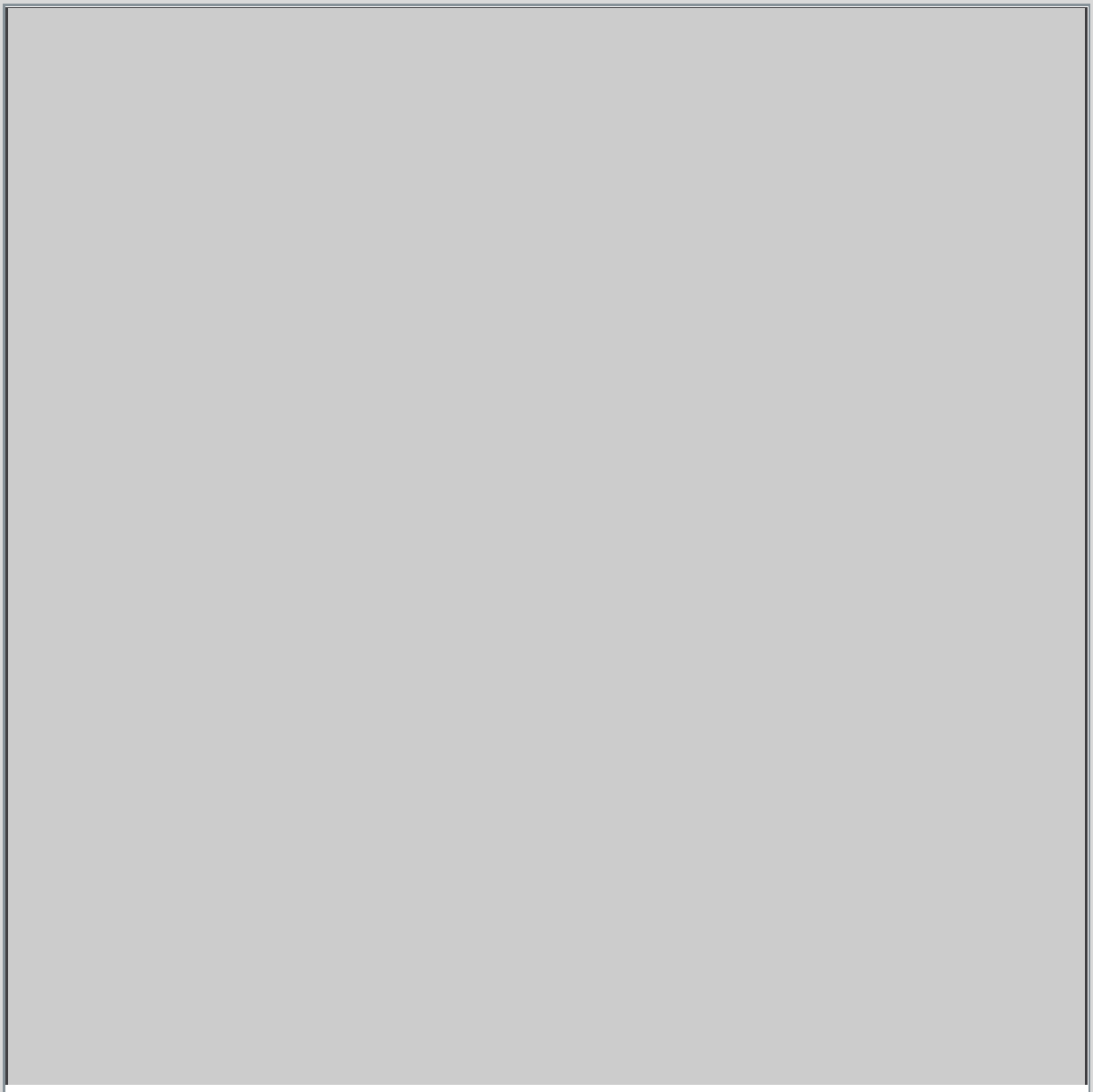
New courses available!

From:	NW3C <training@nw3c.org>
To:	brian.dignan@cookcountyil.gov, Brian Dignan (Sheriff) <Brian.Dignan@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:14 PM CDT
Received:	June 30, 2020 11:10:18 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

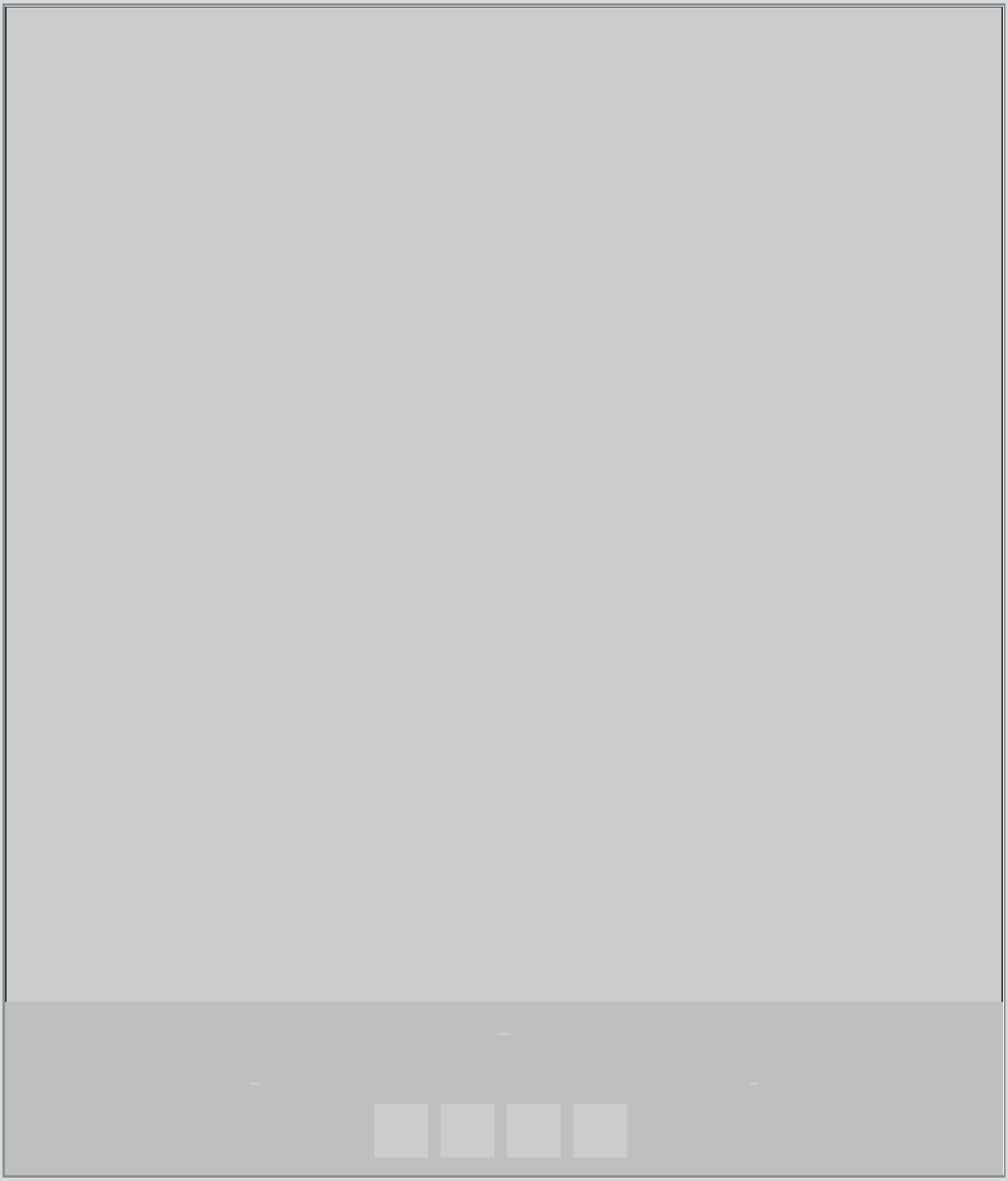
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

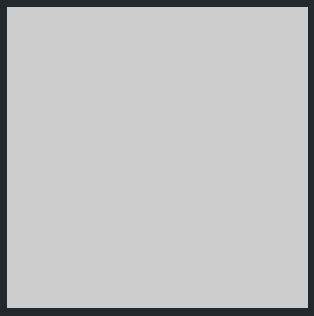
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Daniel Redican (Sheriff)
Sent:	June 30, 2020 11:10:14 PM CDT
Received:	June 30, 2020 11:10:19 PM CDT

New courses available!

To:	Pascal Waller (Sheriff)
Sent:	June 30, 2020 11:10:14 PM CDT
Received:	June 30, 2020 11:10:18 PM CDT

New courses available!

To:	Brian Dignan (Sheriff)
Sent:	June 30, 2020 11:10:14 PM CDT
Received:	June 30, 2020 11:10:18 PM CDT

New courses available!

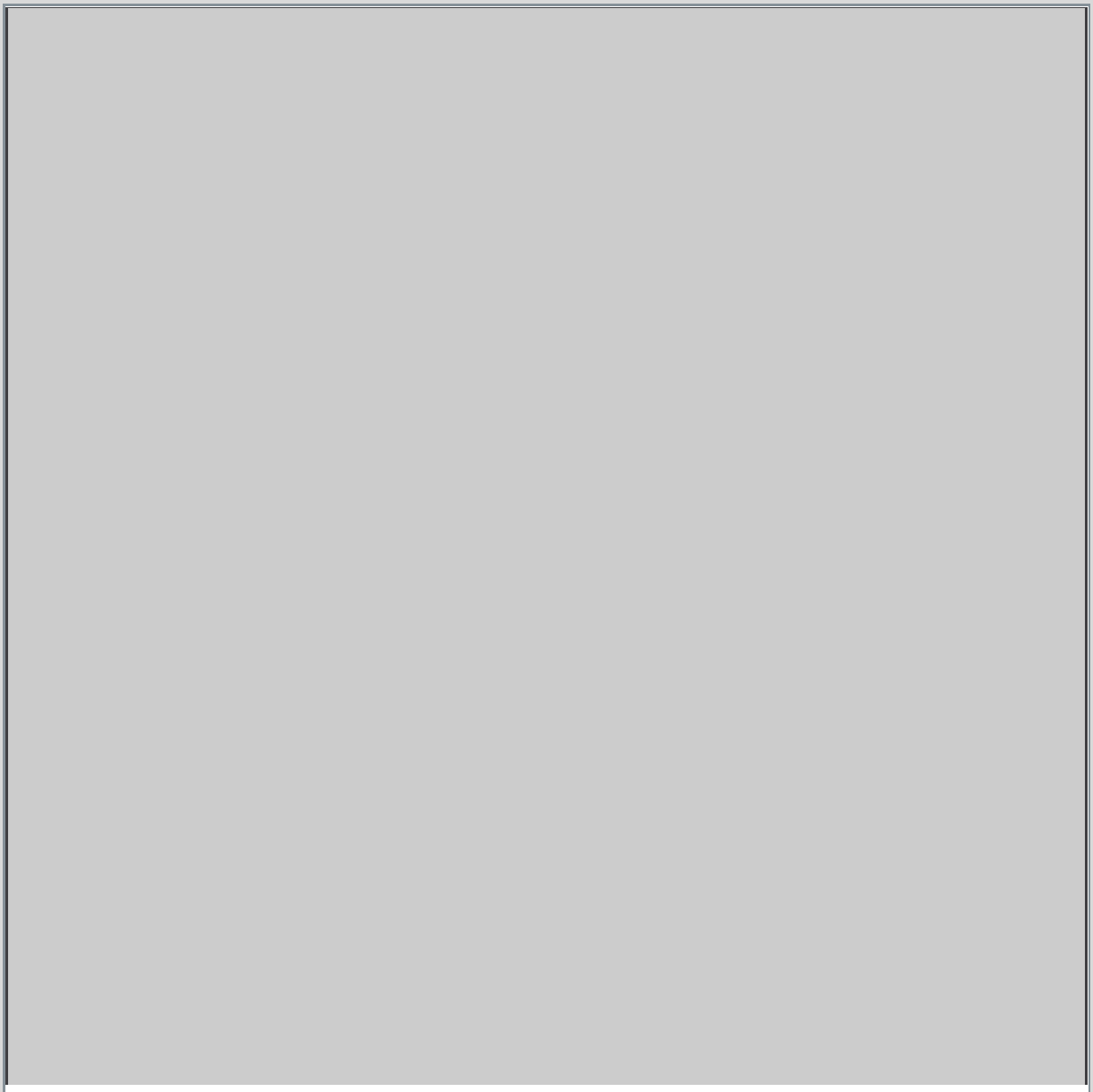
From: NW3C <training@nw3c.org>
To: james.davis@cookcountyil.gov, James Davis (Sheriff) <James.Davis@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:15 PM CDT
Received: June 30, 2020 11:10:19 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

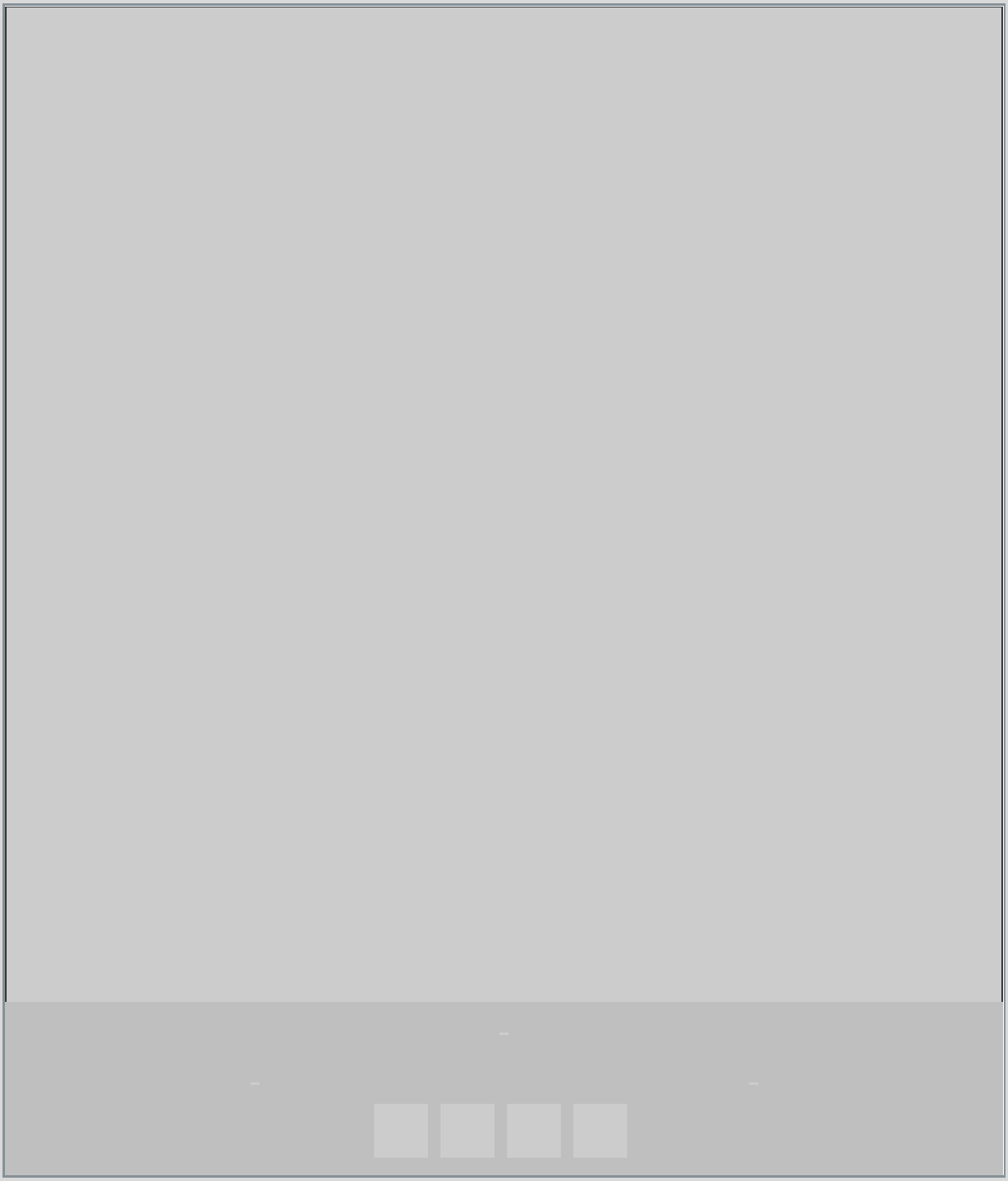
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

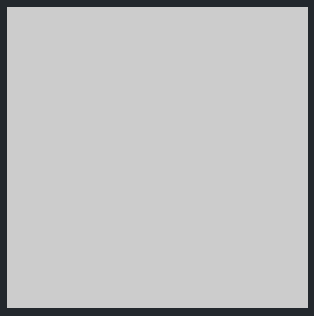
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

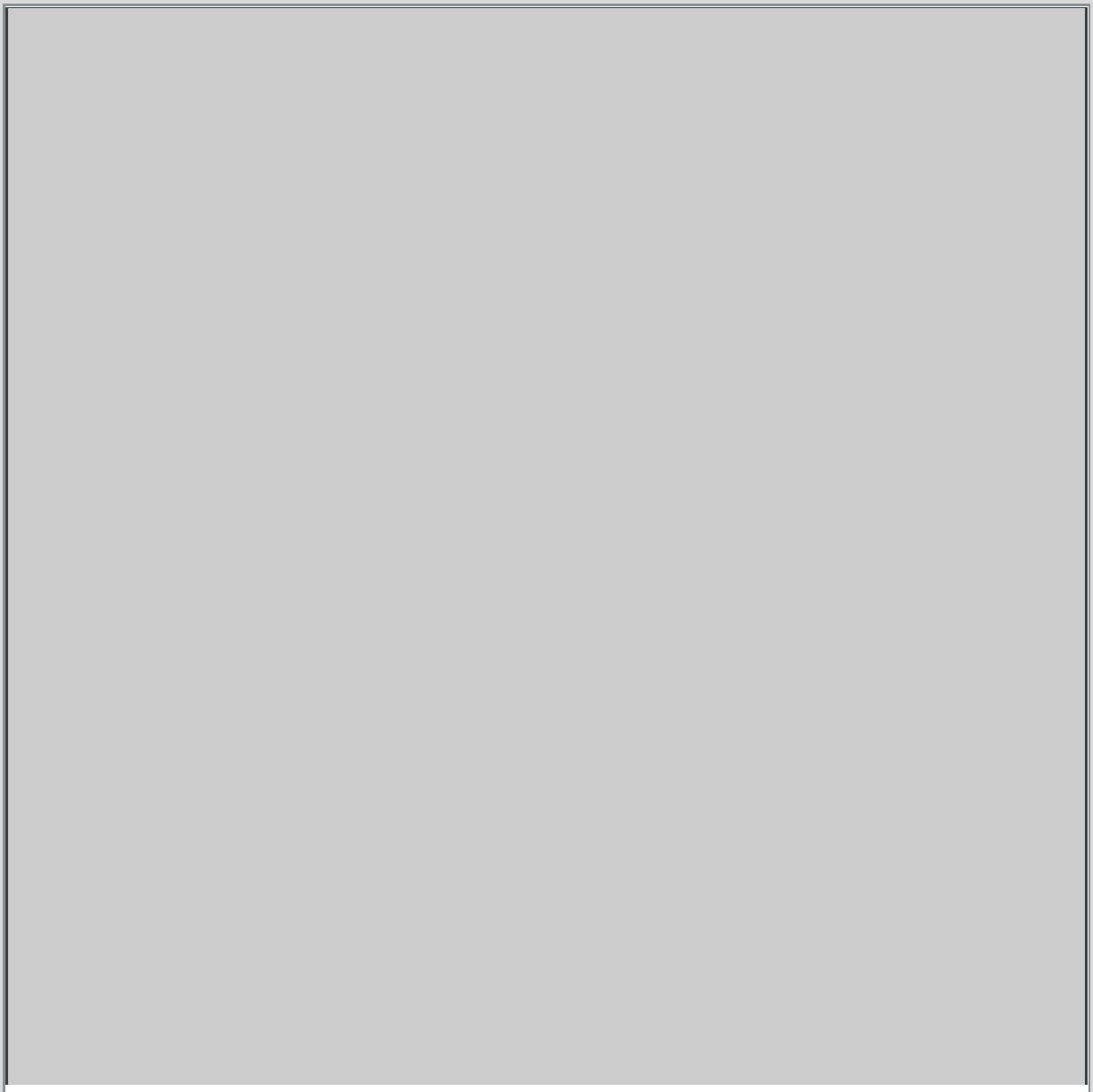
From: NW3C <training@nw3c.org>
To: james.draz@cookcountyil.gov, James Draz (Sheriff) <James.Draz@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:15 PM CDT
Received: June 30, 2020 11:10:20 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

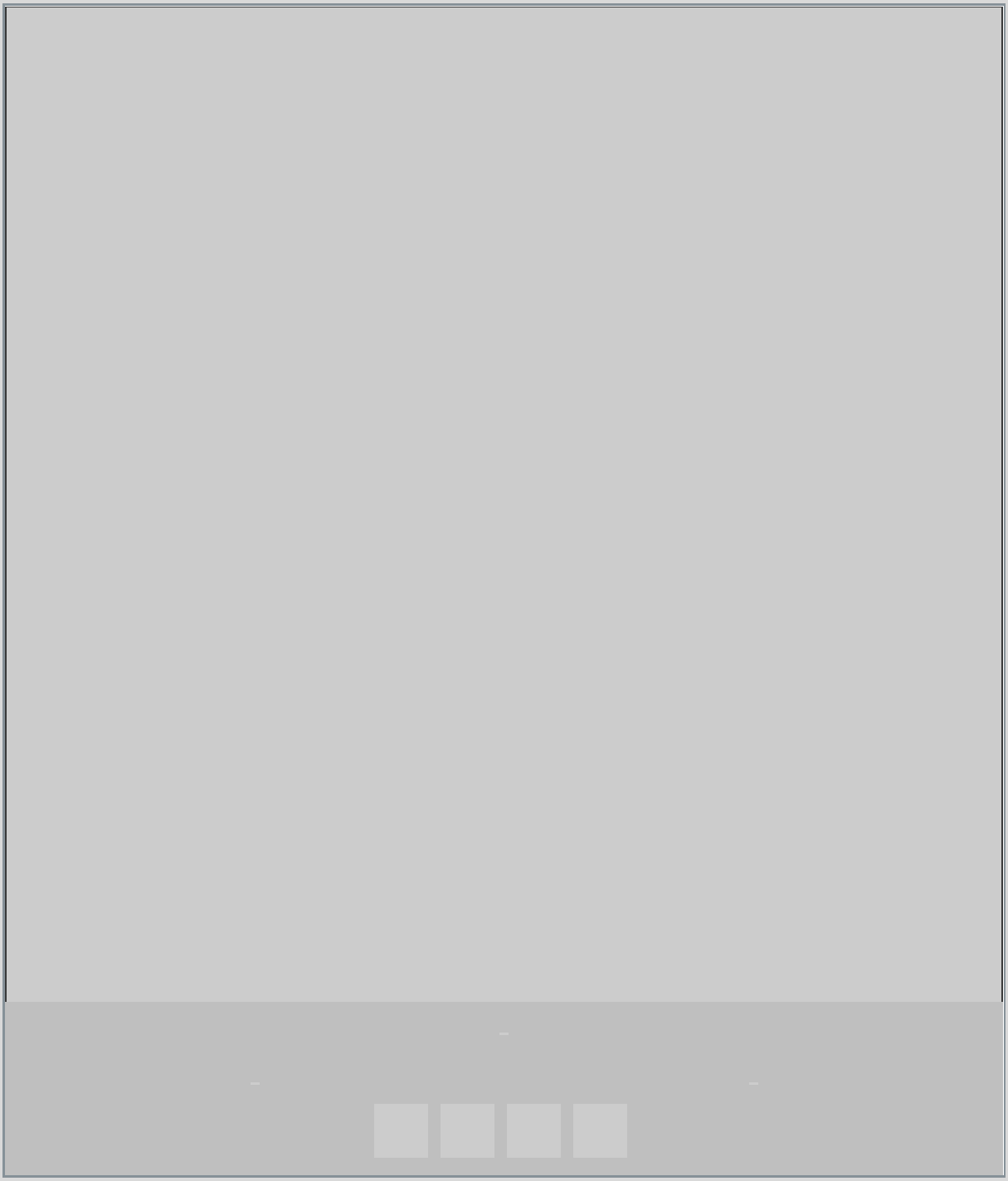
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

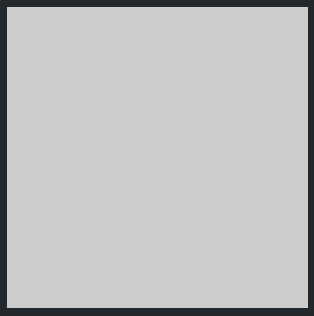
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

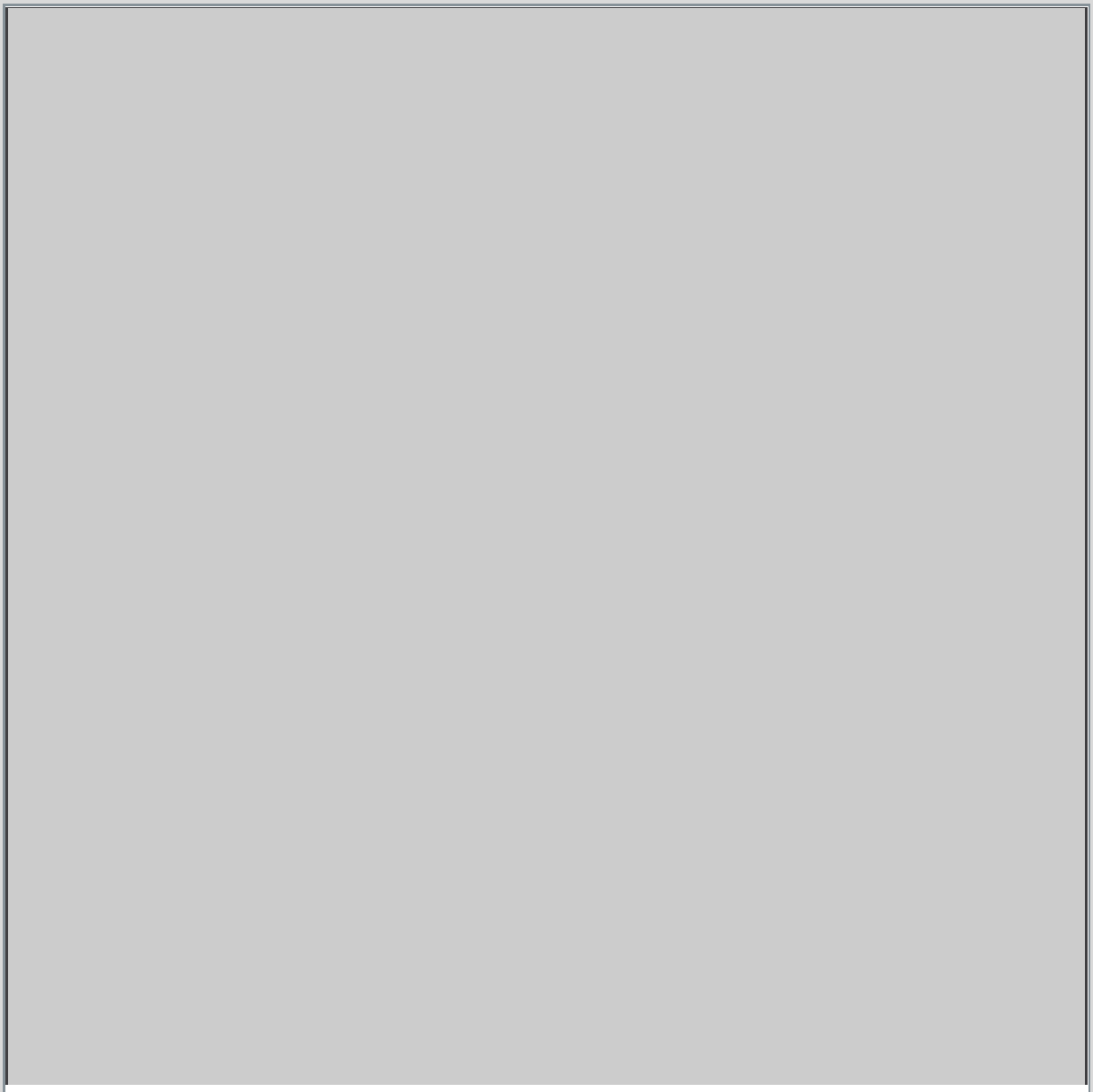
New courses available!

From:	NW3C <training@nw3c.org>
To:	helen.siaj@cookcountyil.gov, Helen Siaj (Sheriff) <Helen.Siaj@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:15 PM CDT
Received:	June 30, 2020 11:10:17 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

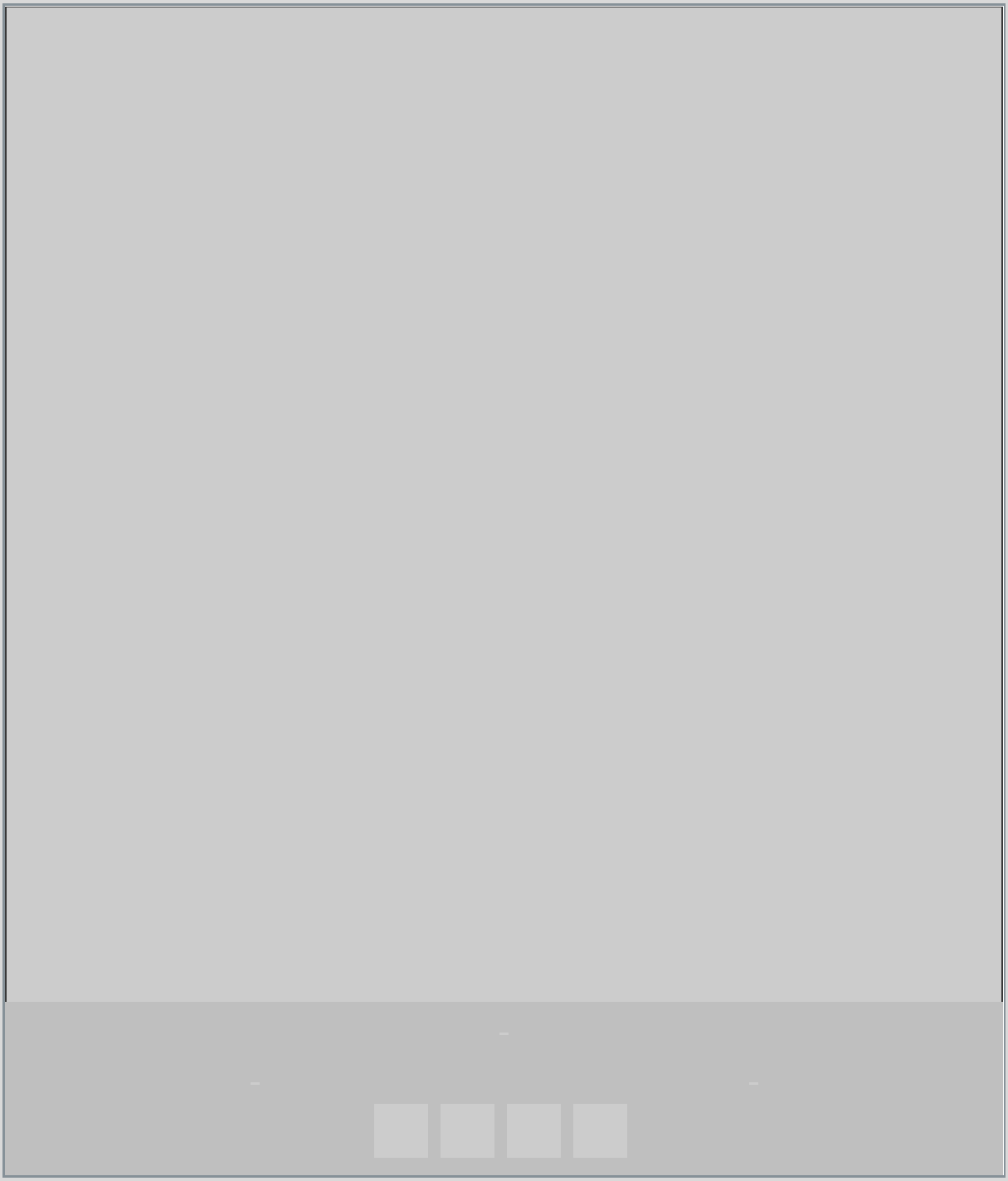
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

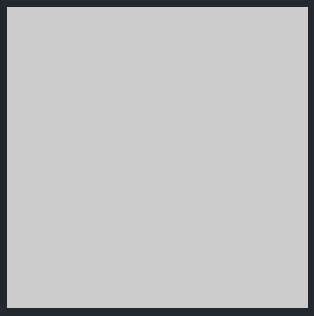
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	James Davis (Sheriff)
Sent:	June 30, 2020 11:10:15 PM CDT
Received:	June 30, 2020 11:10:20 PM CDT

New courses available!

To:	James Draz (Sheriff)
Sent:	June 30, 2020 11:10:15 PM CDT
Received:	June 30, 2020 11:10:20 PM CDT

New courses available!

To:	Helen Siaj (Sheriff)
Sent:	June 30, 2020 11:10:15 PM CDT
Received:	June 30, 2020 11:10:25 PM CDT

New courses available!

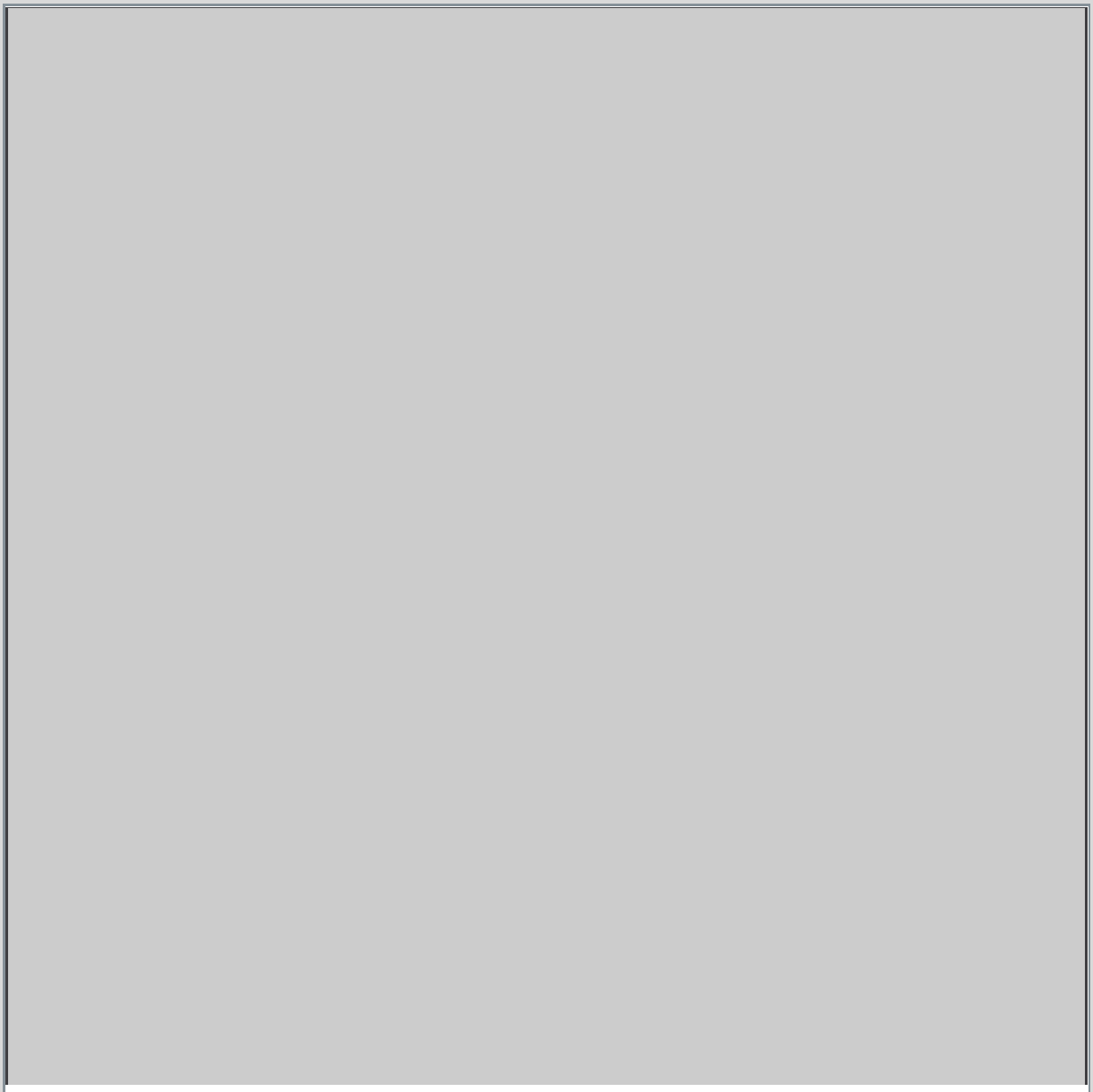
From: NW3C <training@nw3c.org>
To: nelson.lewis@cookcountyil.gov, Nelson Lewis (Sheriff) <Nelson.Lewis@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:17 PM CDT
Received: June 30, 2020 11:10:19 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

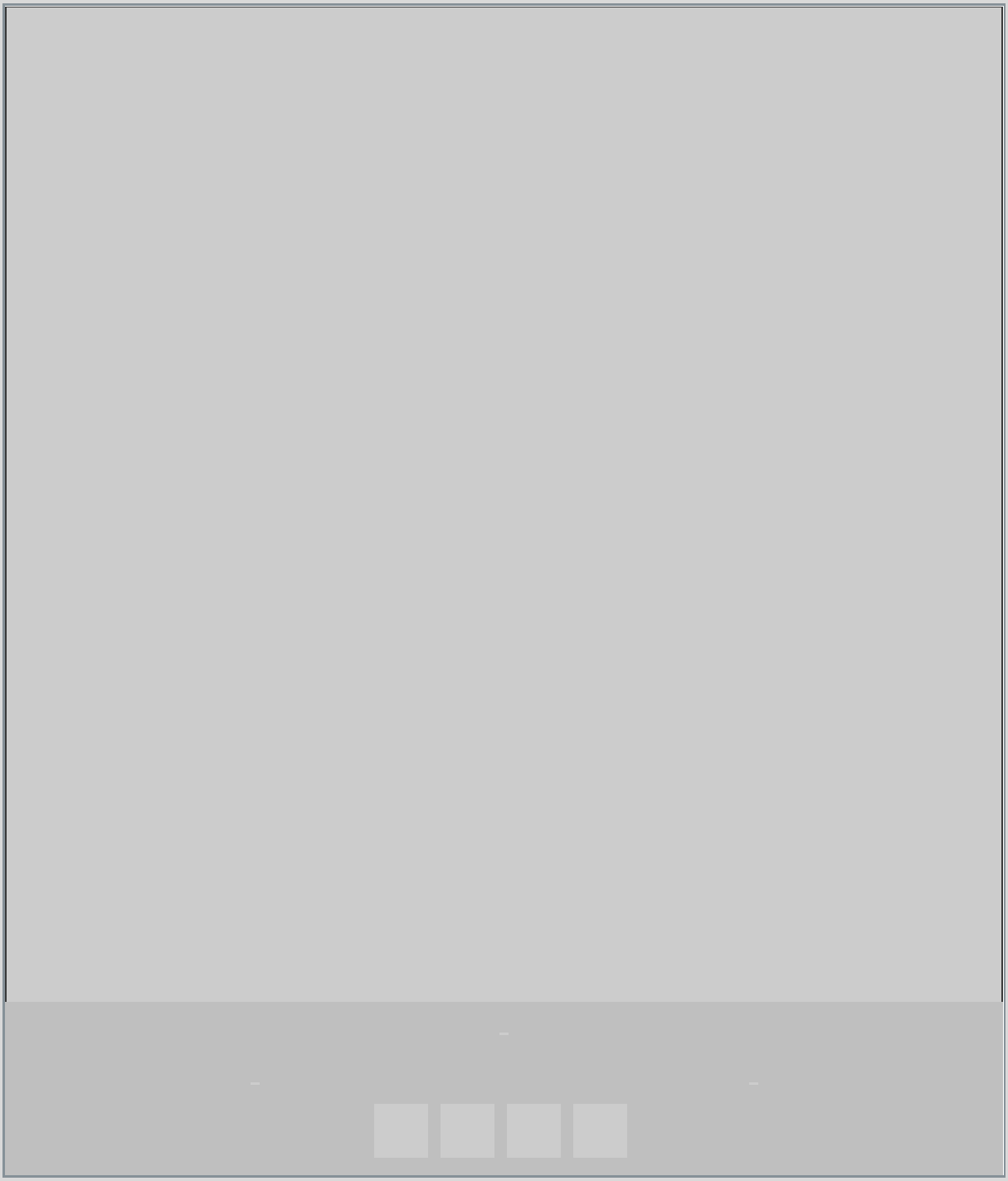
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

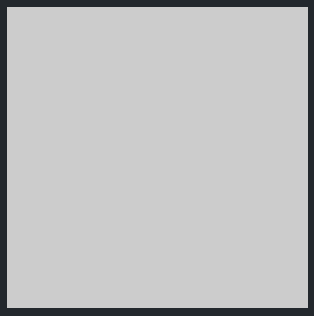
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Nelson Lewis (Sheriff)
Sent:	June 30, 2020 11:10:17 PM CDT
Received:	June 30, 2020 11:10:20 PM CDT

New courses available!

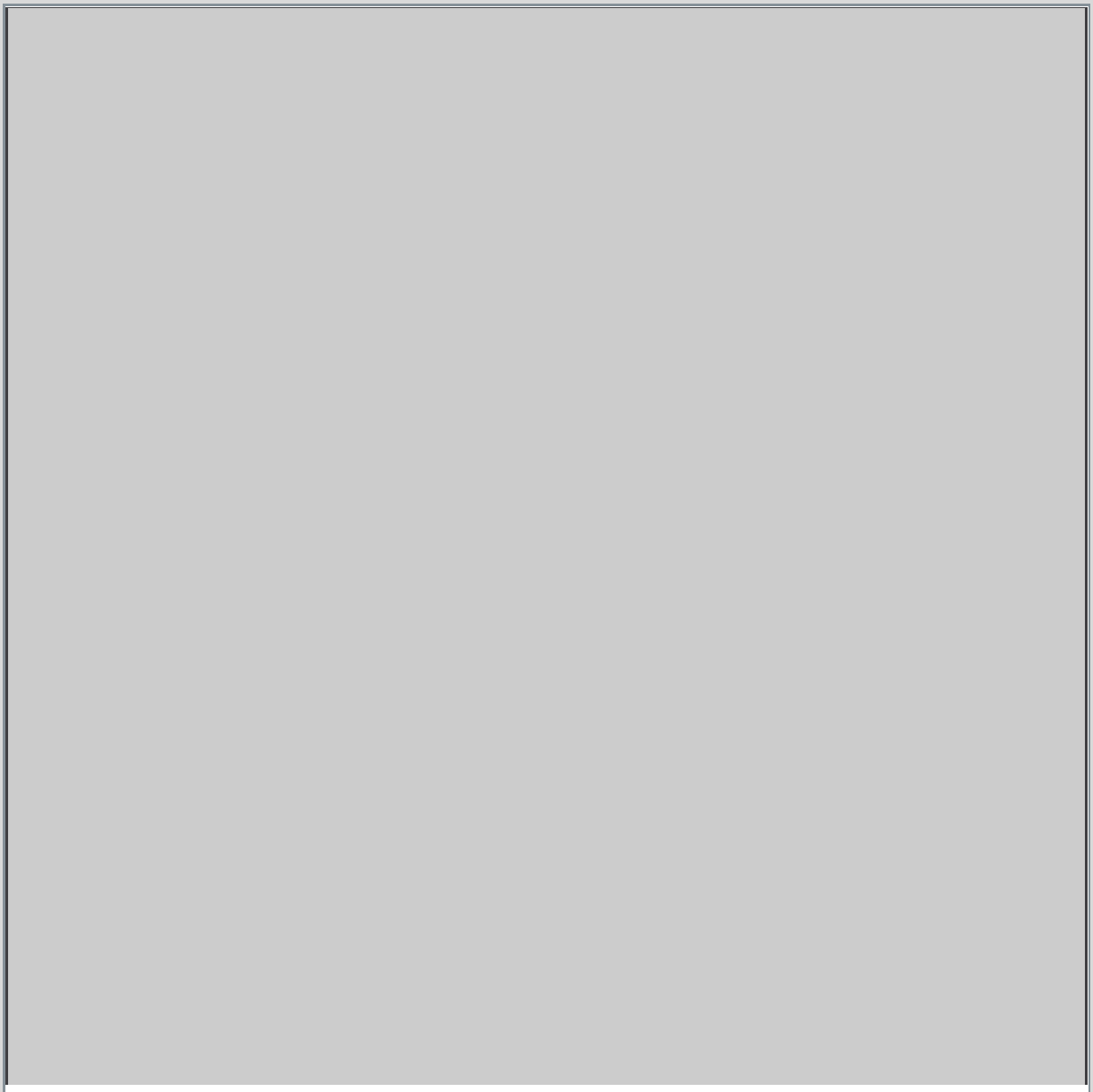
From: NW3C <training@nw3c.org>
To: darryl.ashley@cookcountyil.gov, Darryl Ashley (Sheriff) <Darryl.Ashley@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:21 PM CDT
Received: June 30, 2020 11:10:25 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

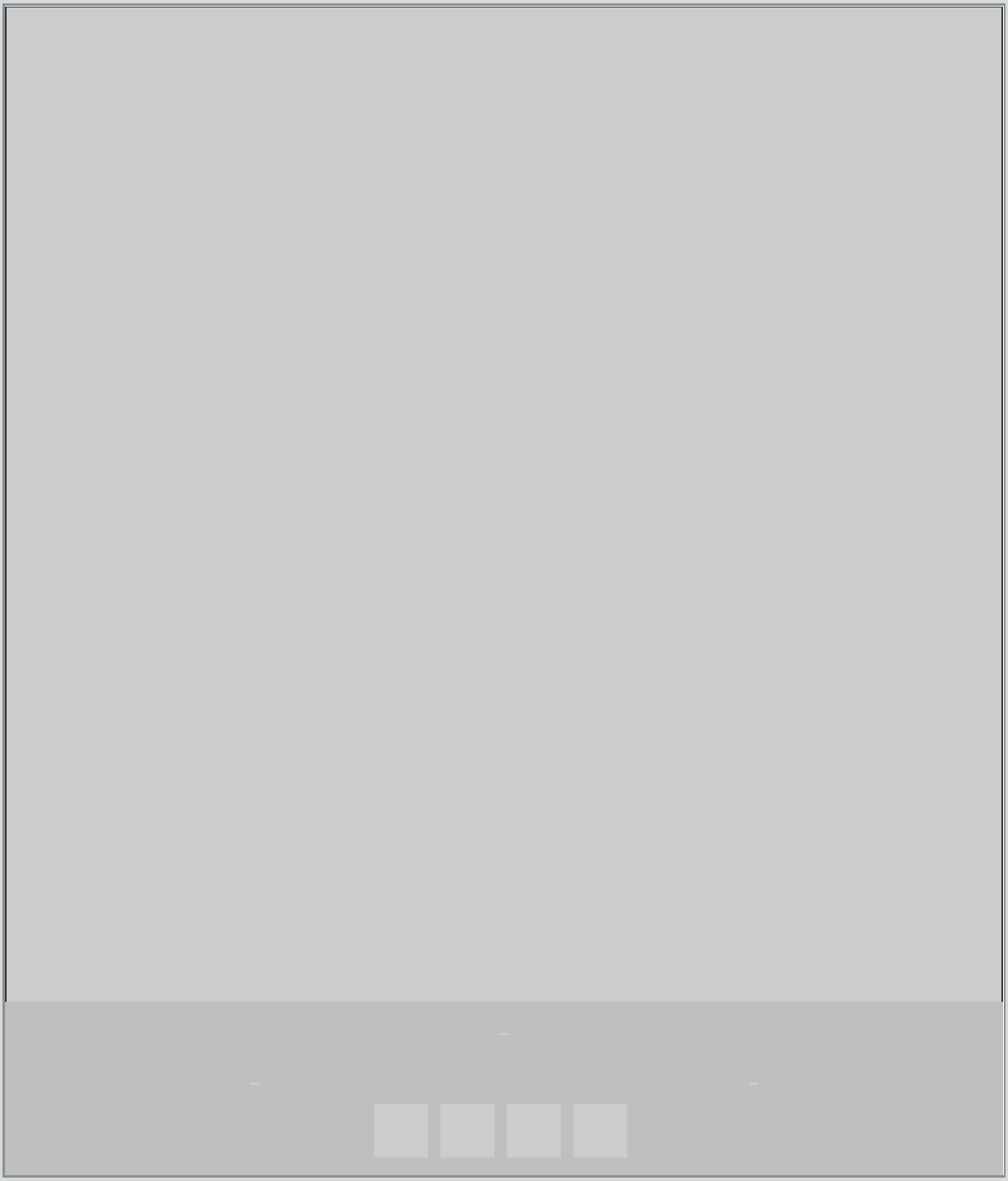
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

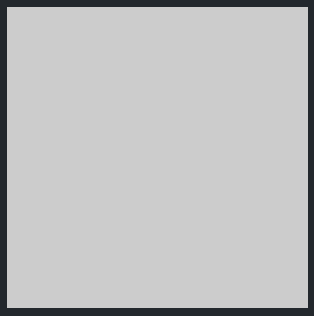
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Darryl Ashley (Sheriff)
Sent:	June 30, 2020 11:10:21 PM CDT
Received:	June 30, 2020 11:10:25 PM CDT

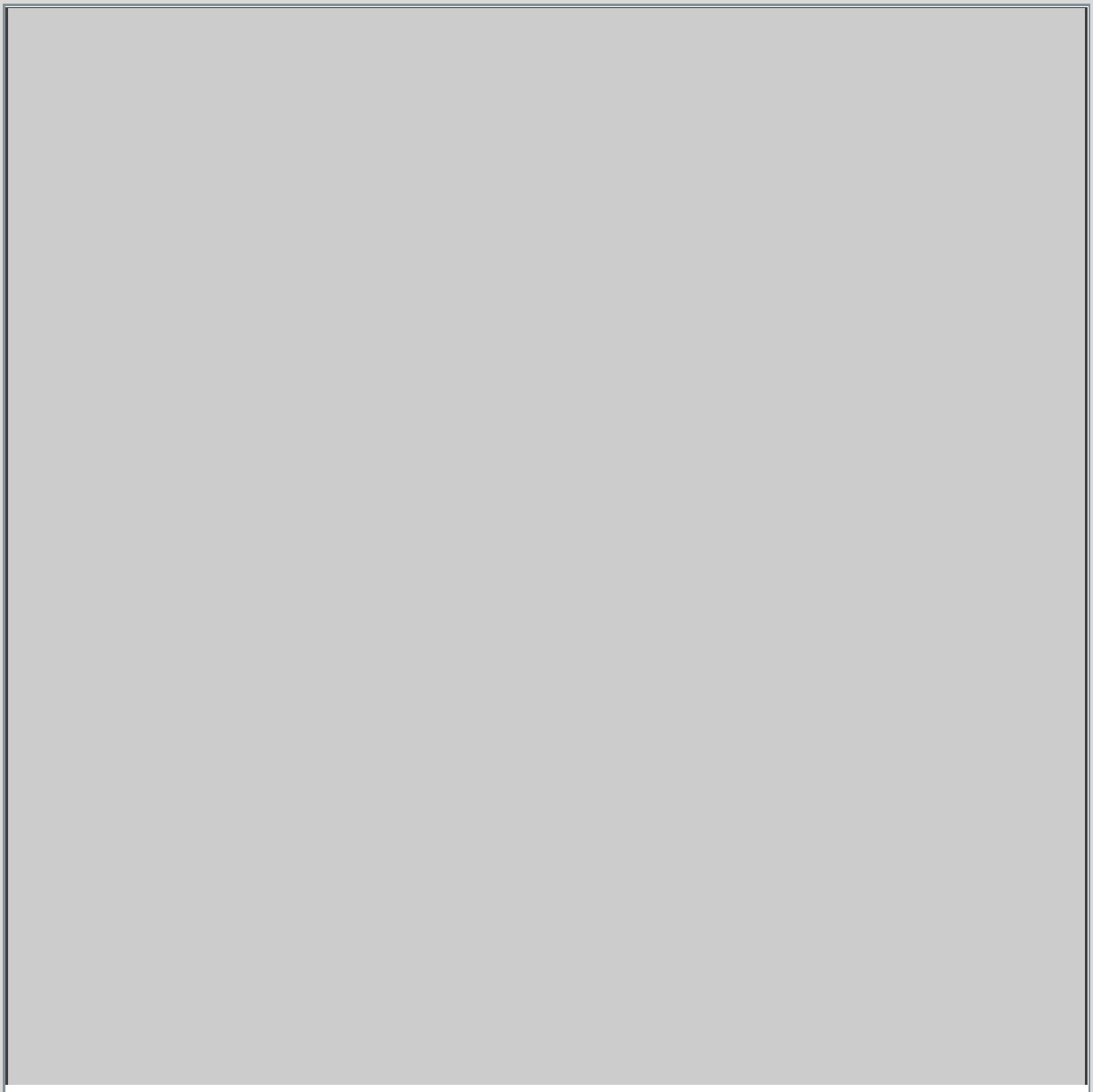
New courses available!

From:	NW3C <training@nw3c.org>
To:	timothy.mcphillips@cookcountyil.gov, Timothy McPhillips (Sheriff) <Timothy.Mcphillips@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:22 PM CDT
Received:	June 30, 2020 11:10:24 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

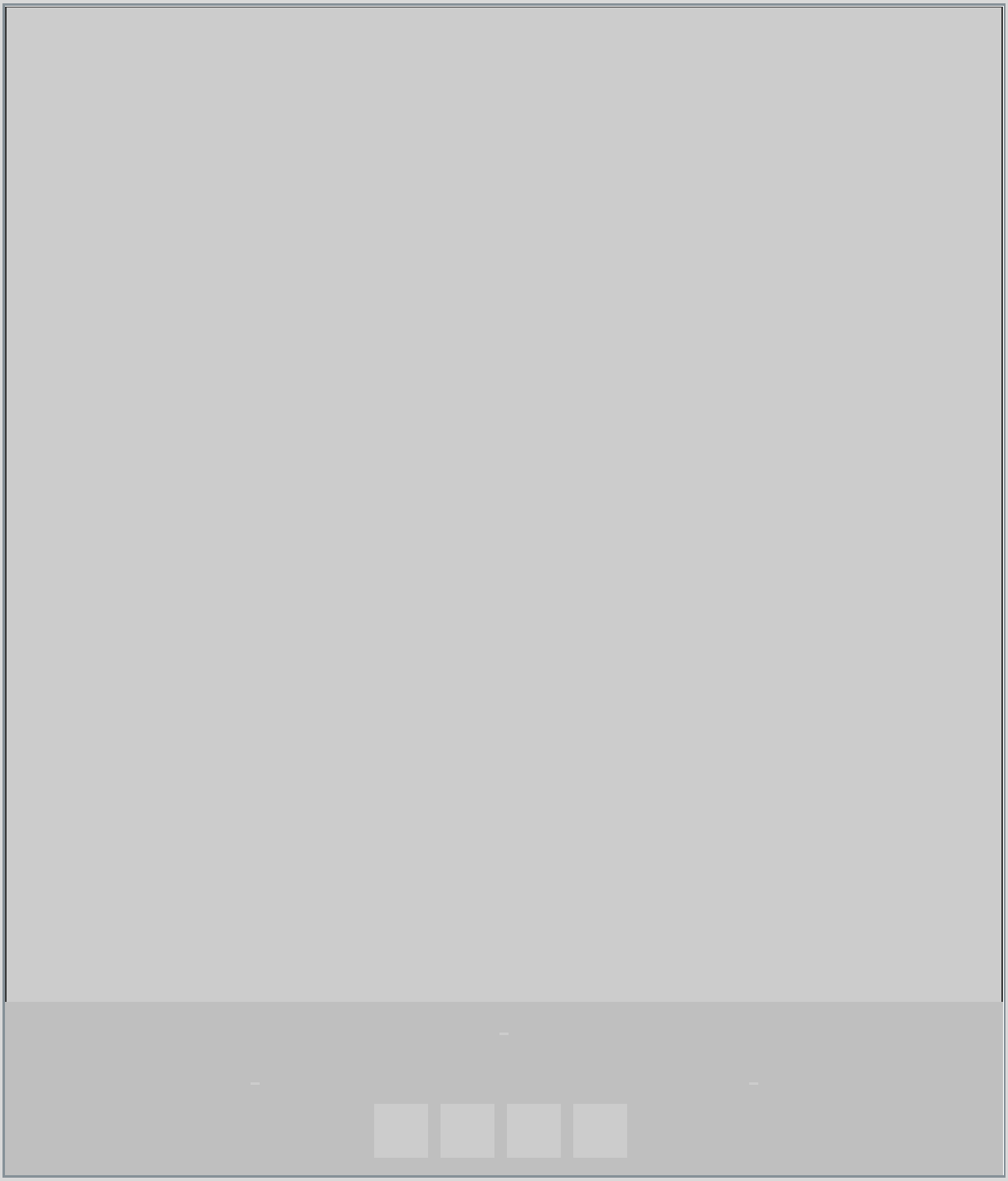
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

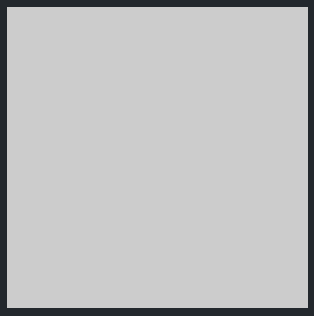
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Timothy McPhillips (Sheriff)
Sent:	June 30, 2020 11:10:22 PM CDT
Received:	June 30, 2020 11:10:25 PM CDT

New courses available!

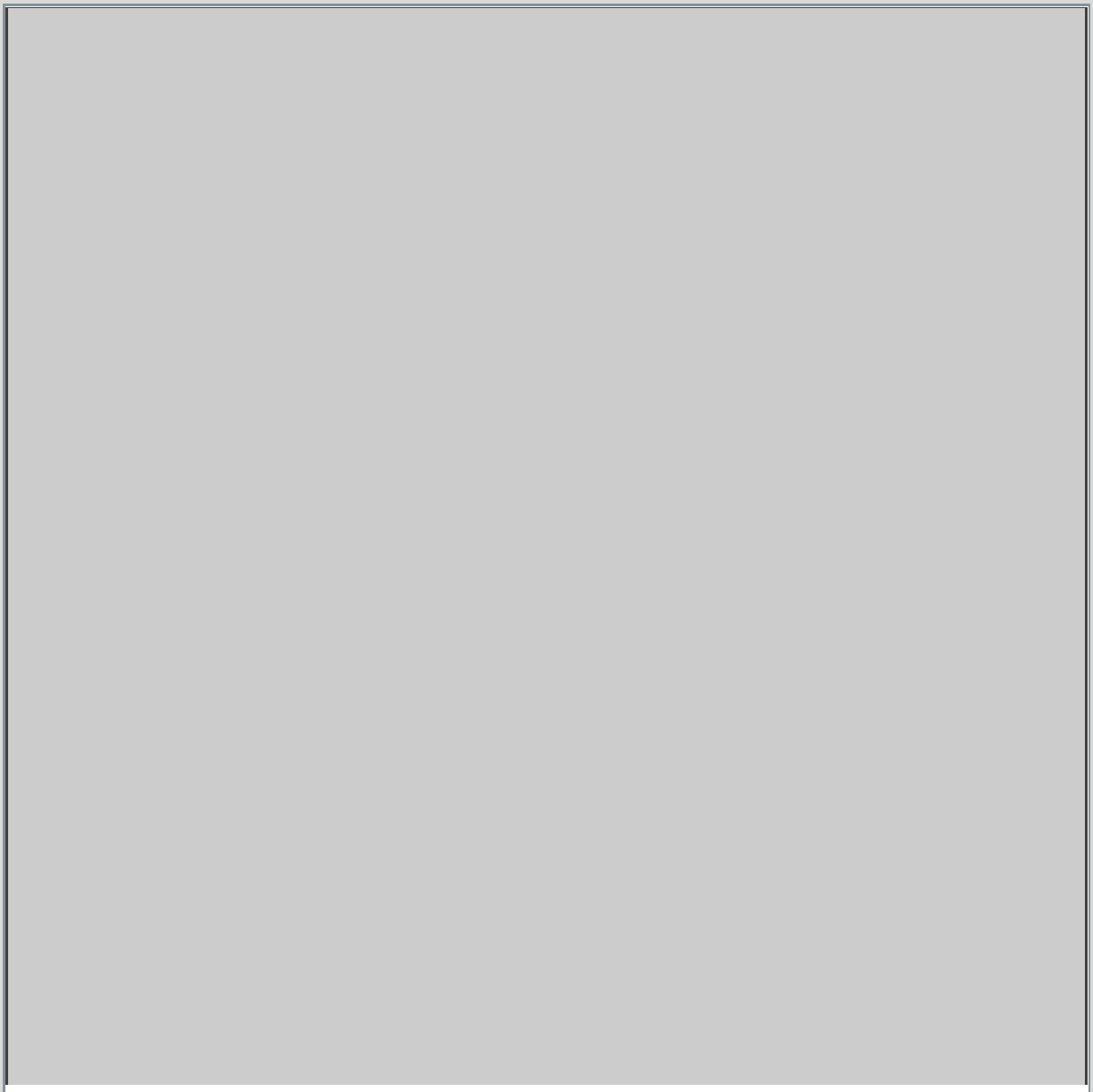
From: NW3C <training@nw3c.org>
To: marguerite.mccluskey@cookcountyil.gov, Marguerite McCluskey (Sheriff) <Marguerite.McCluskey@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:24 PM CDT
Received: June 30, 2020 11:10:26 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

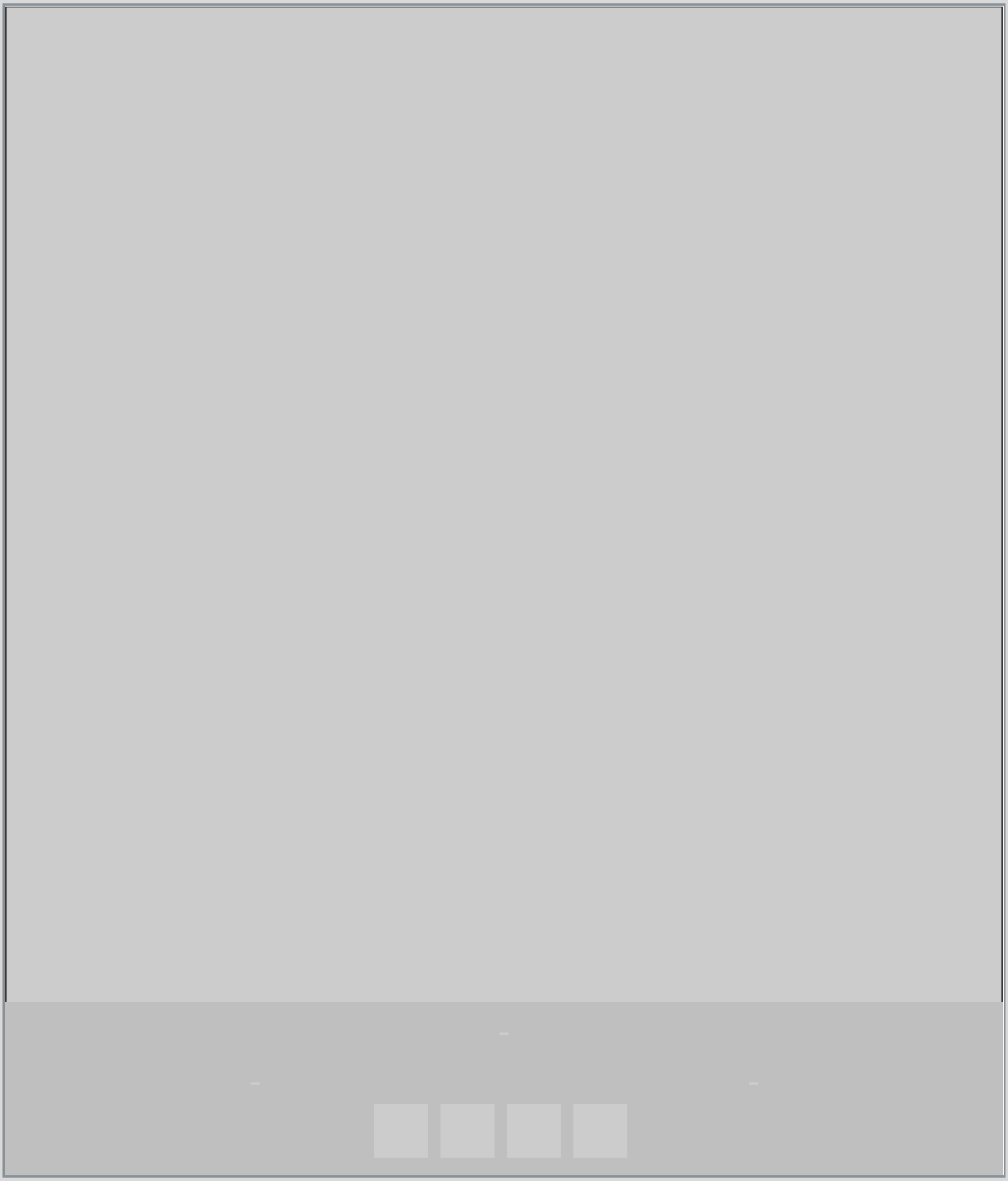
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

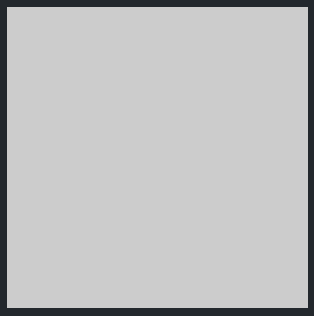
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Marguerite McCluskey (Sheriff)
Sent:	June 30, 2020 11:10:24 PM CDT
Received:	June 30, 2020 11:10:27 PM CDT

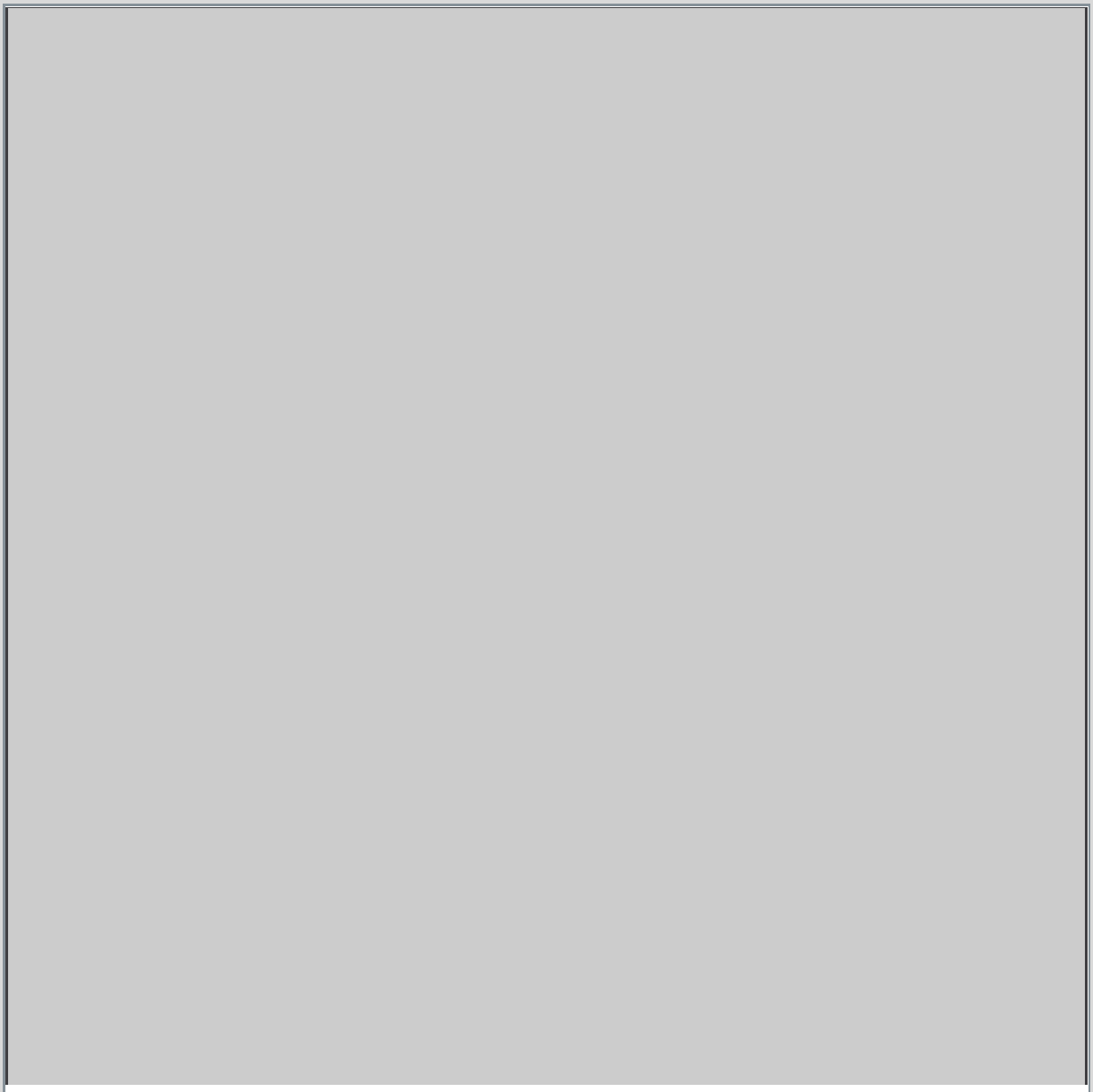
New courses available!

From:	NW3C <training@nw3c.org>
To:	brandon.ducray@cookcountyil.gov, Brandon Ducray (Sheriff) <Brandon.Ducray@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:25 PM CDT
Received:	June 30, 2020 11:10:28 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

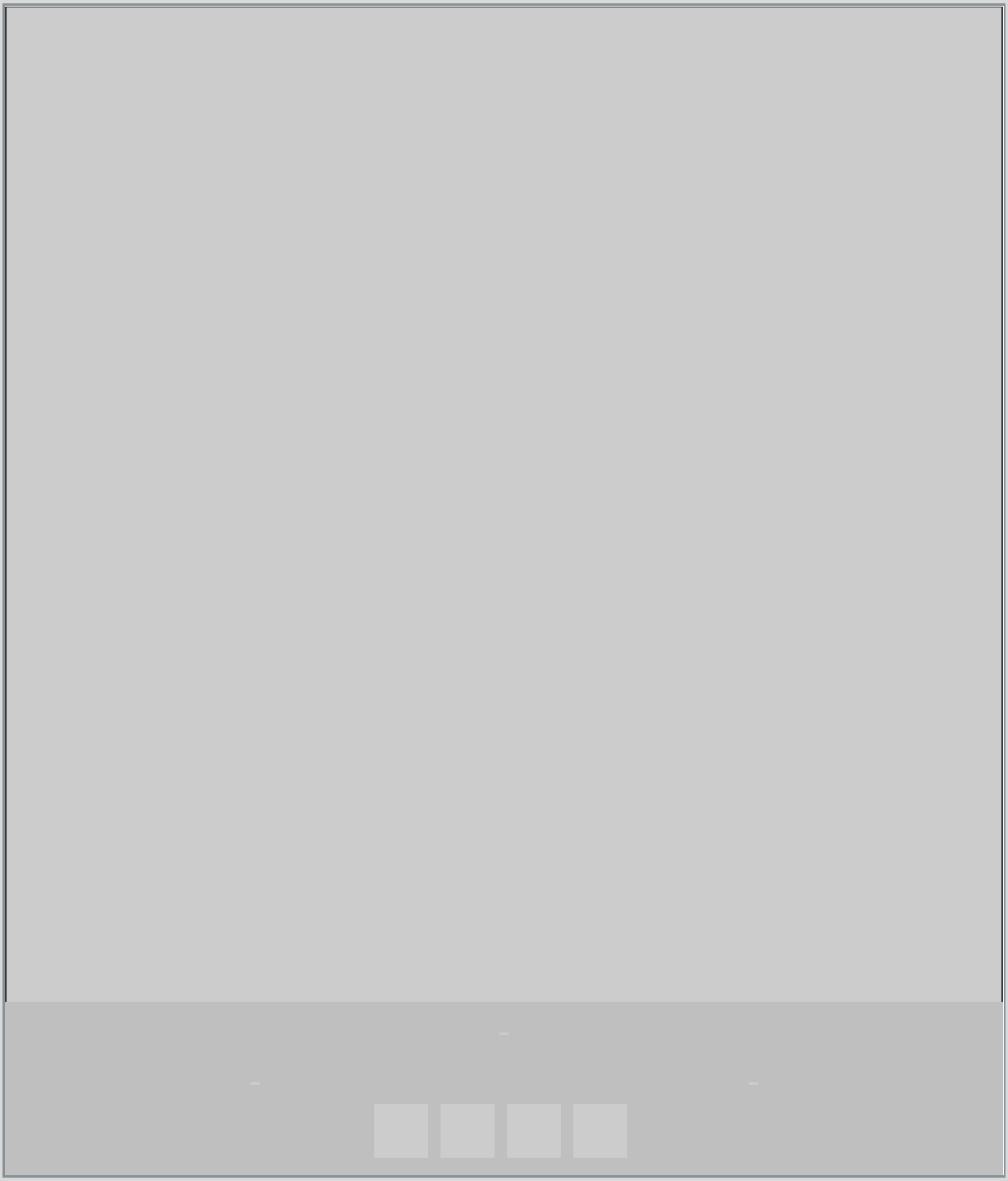
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

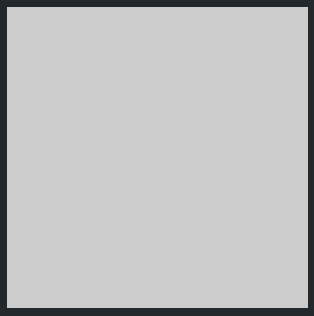
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

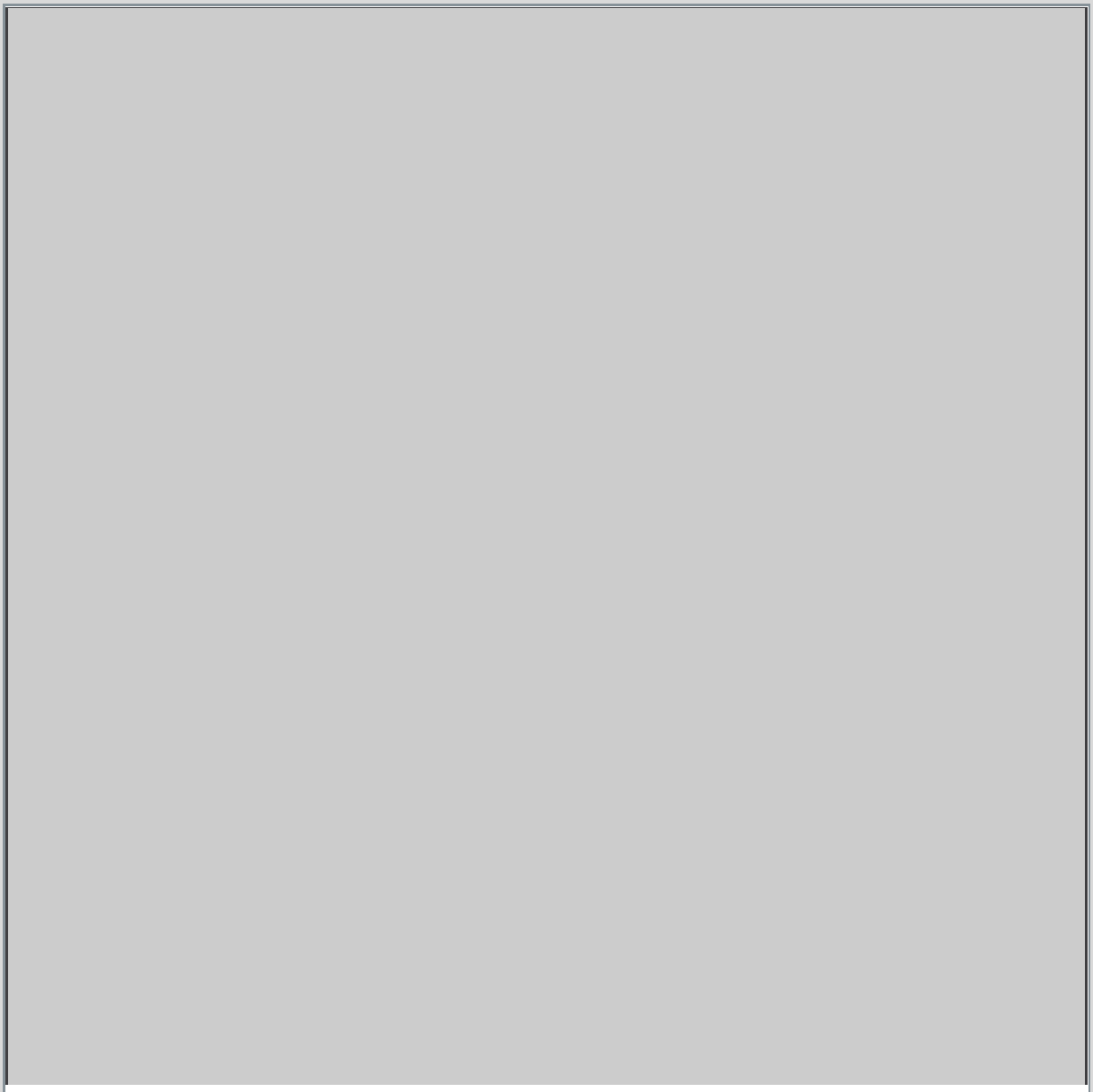
From: NW3C <training@nw3c.org>
To: patrick.doyle@cookcountyil.gov, Patrick Doyle (Sheriff) <Patrick.Doyle@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:25 PM CDT
Received: June 30, 2020 11:10:27 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

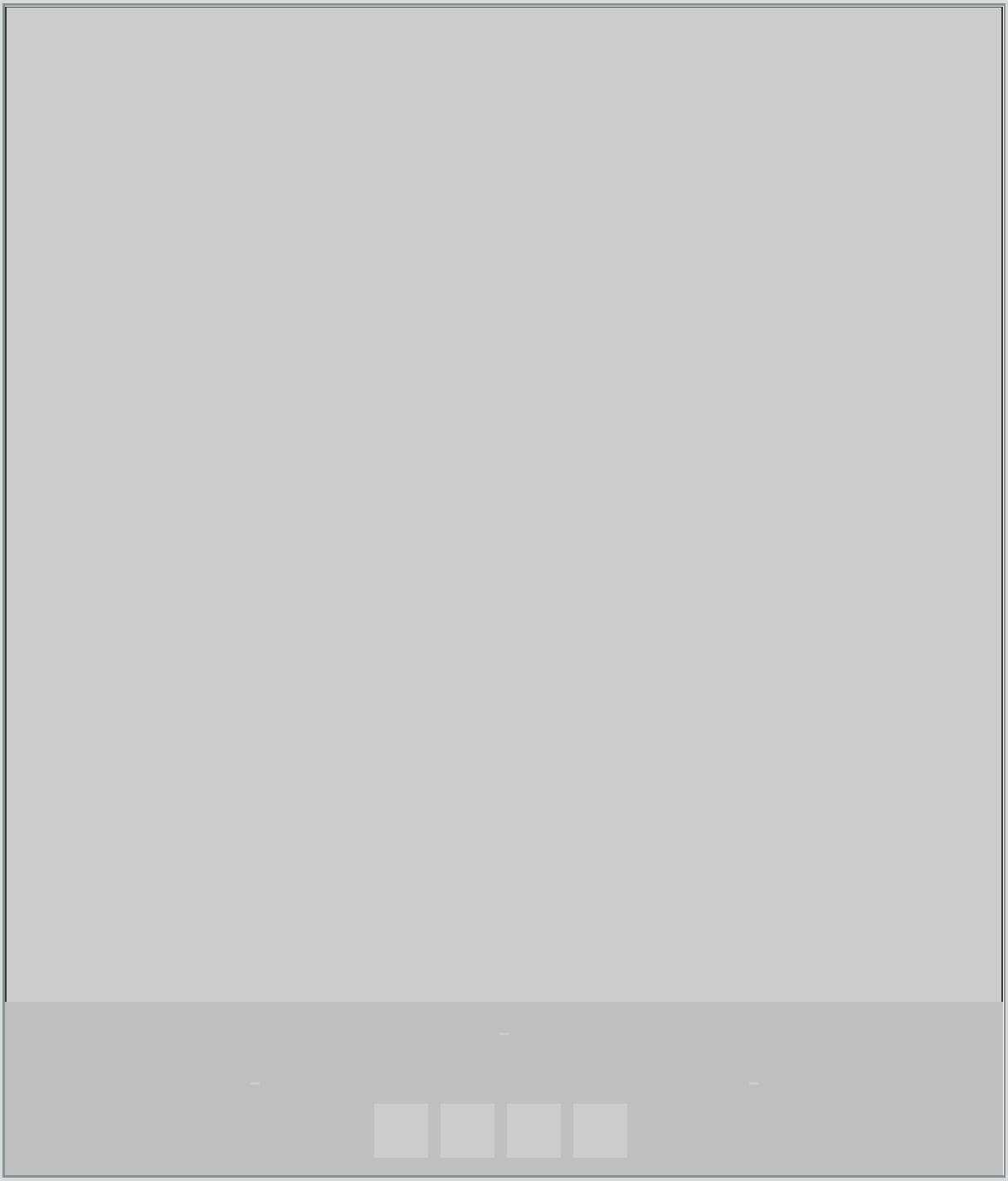
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

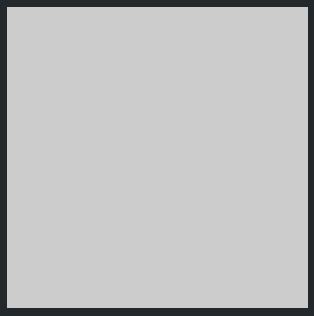
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Brandon Ducray (Sheriff)
Sent:	June 30, 2020 11:10:25 PM CDT
Received:	June 30, 2020 11:10:28 PM CDT

New courses available!

To:	Patrick Doyle (Sheriff)
Sent:	June 30, 2020 11:10:25 PM CDT
Received:	June 30, 2020 11:10:27 PM CDT

New courses available!

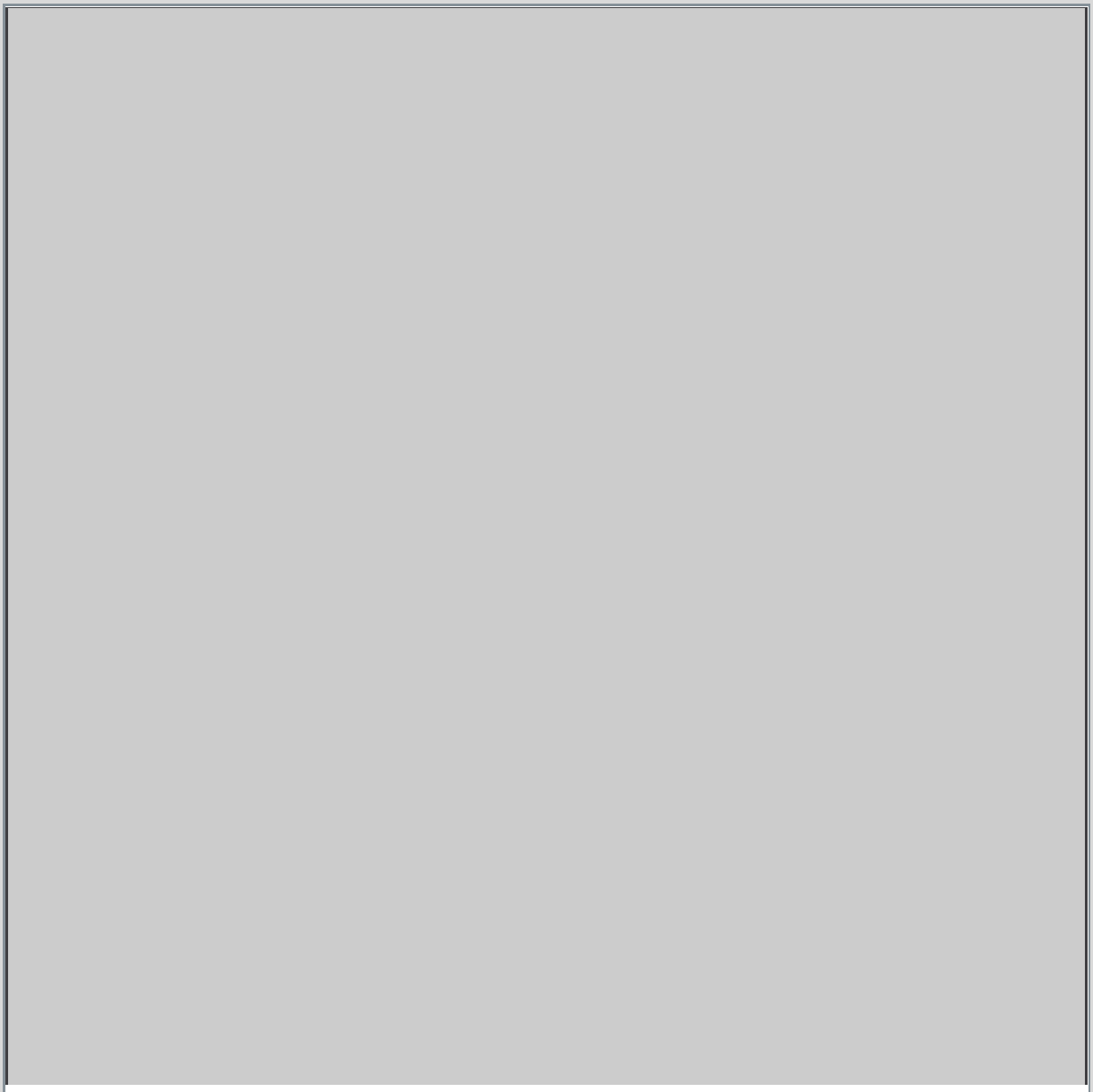
From: NW3C <training@nw3c.org>
To: john.dziedzic@cookcountyil.gov, John Dziedzic (Sheriff) <John.Dziedzic@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:26 PM CDT
Received: June 30, 2020 11:10:29 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

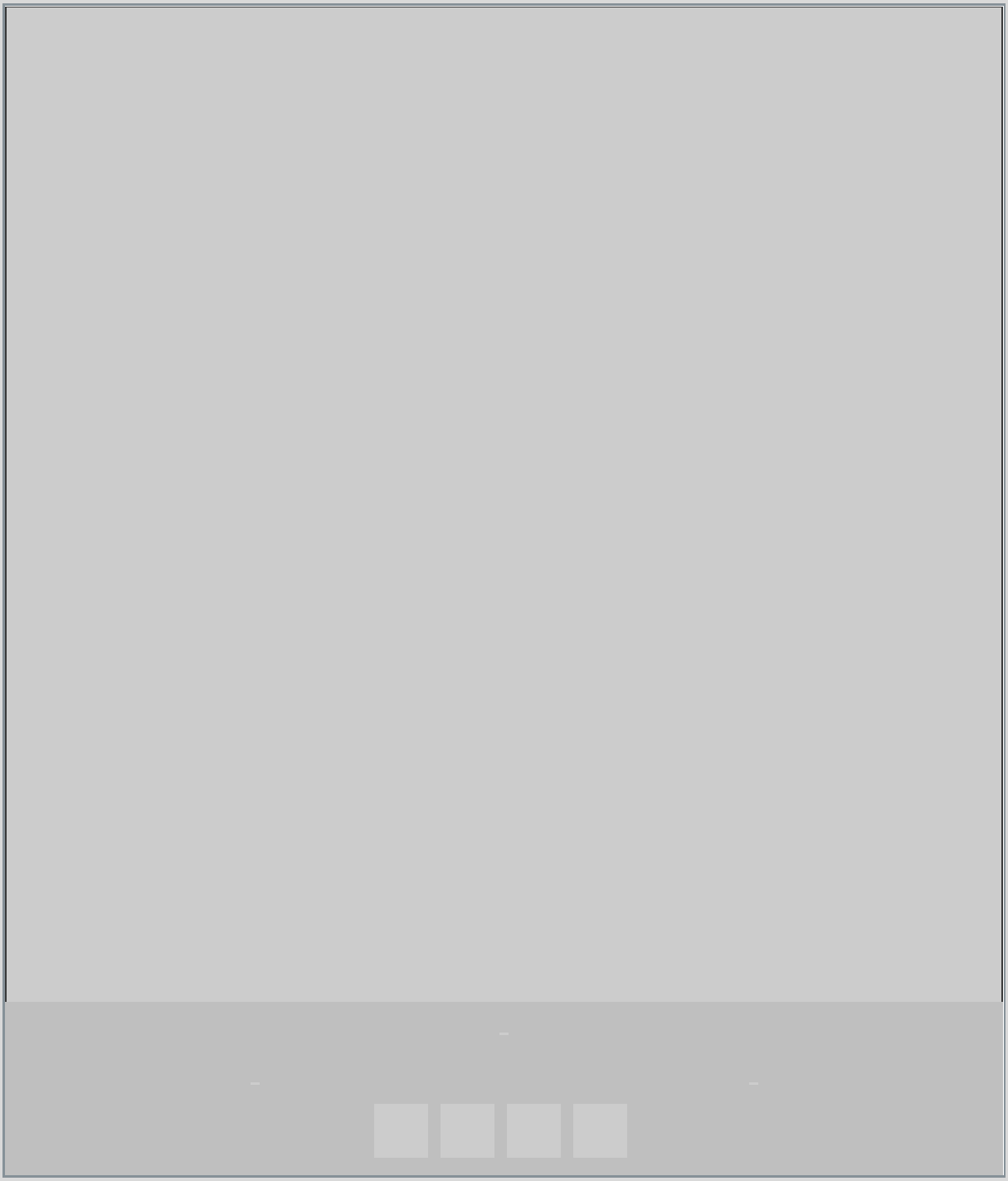
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

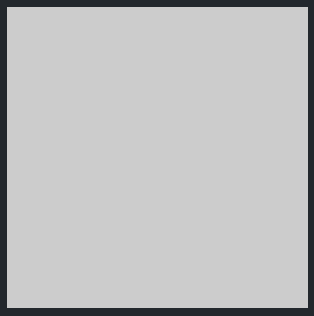
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

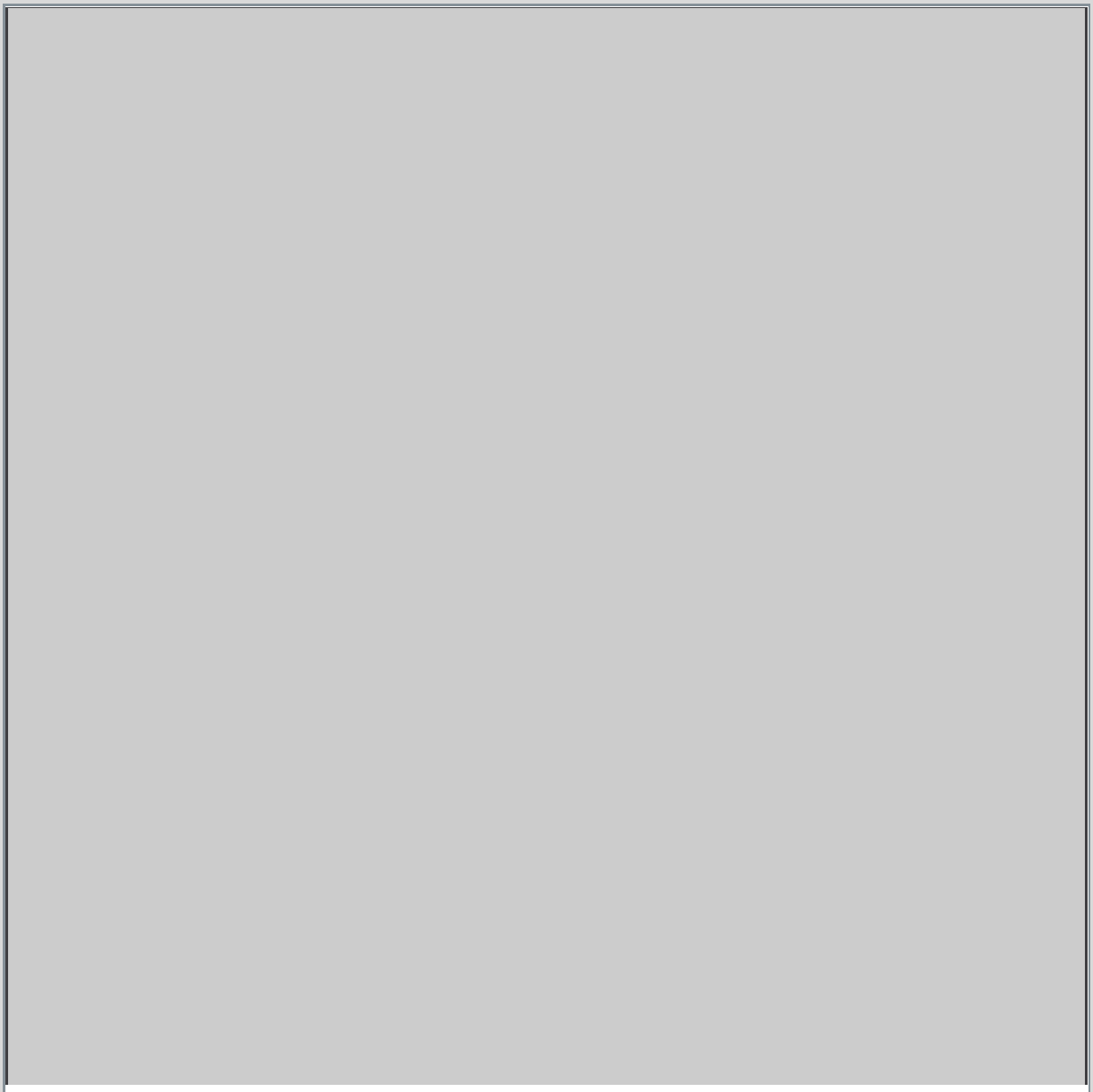
New courses available!

From:	NW3C <training@nw3c.org>
To:	ronald.sachtleben@cookcountyil.gov, Ronald Sachtleben (Sheriff) <Ronald.Sachtleben@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:26 PM CDT
Received:	June 30, 2020 11:10:32 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

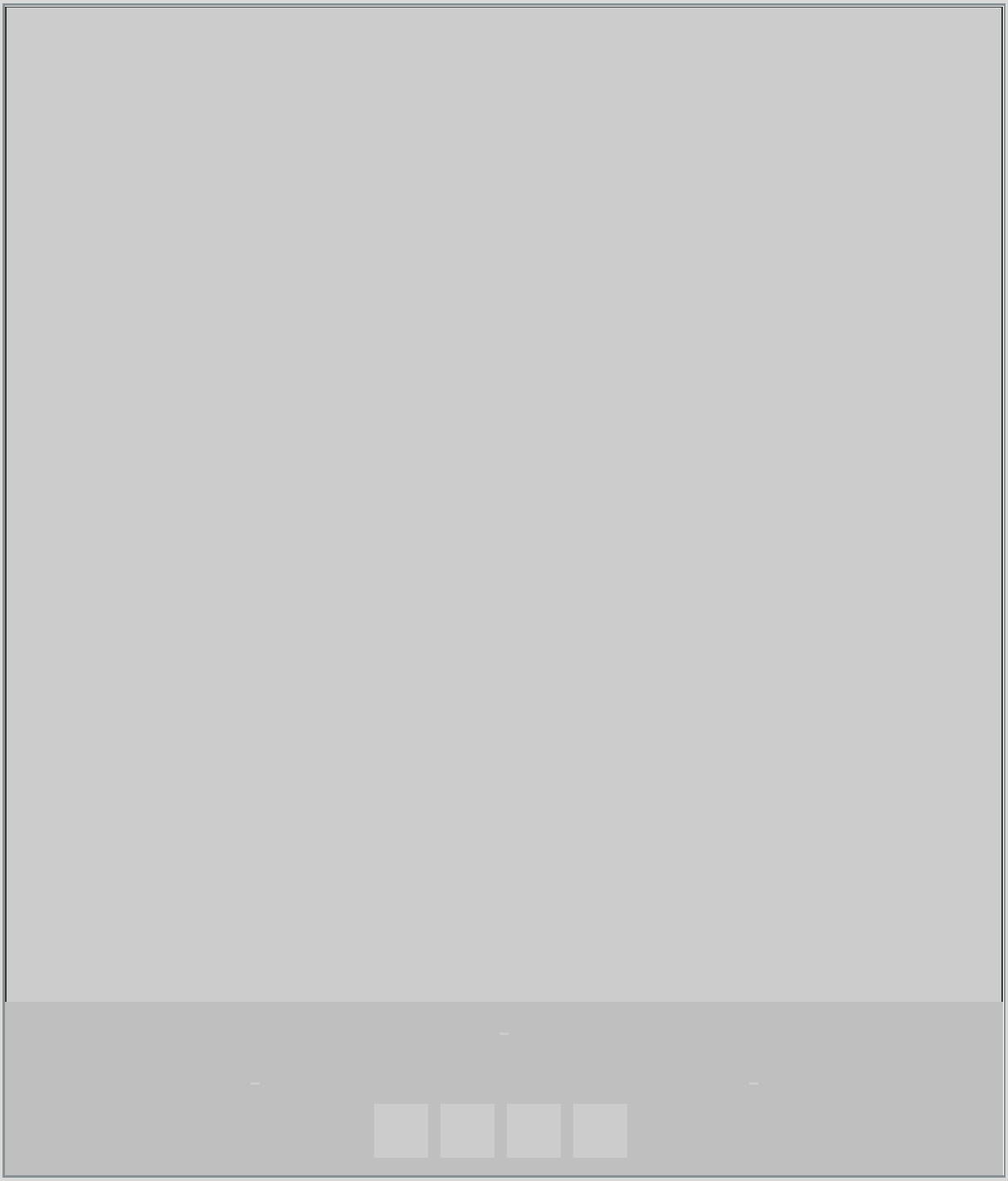
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

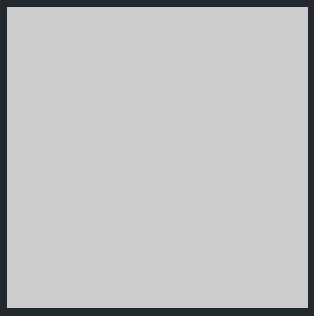
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	John Dziedzic (Sheriff)
Sent:	June 30, 2020 11:10:26 PM CDT
Received:	June 30, 2020 11:10:30 PM CDT

New courses available!

To:	Ronald Sachtleben (Sheriff), 2020 Criminal Investigations Supervisors
Sent:	June 30, 2020 11:10:26 PM CDT
Received:	June 30, 2020 11:10:32 PM CDT

New courses available!

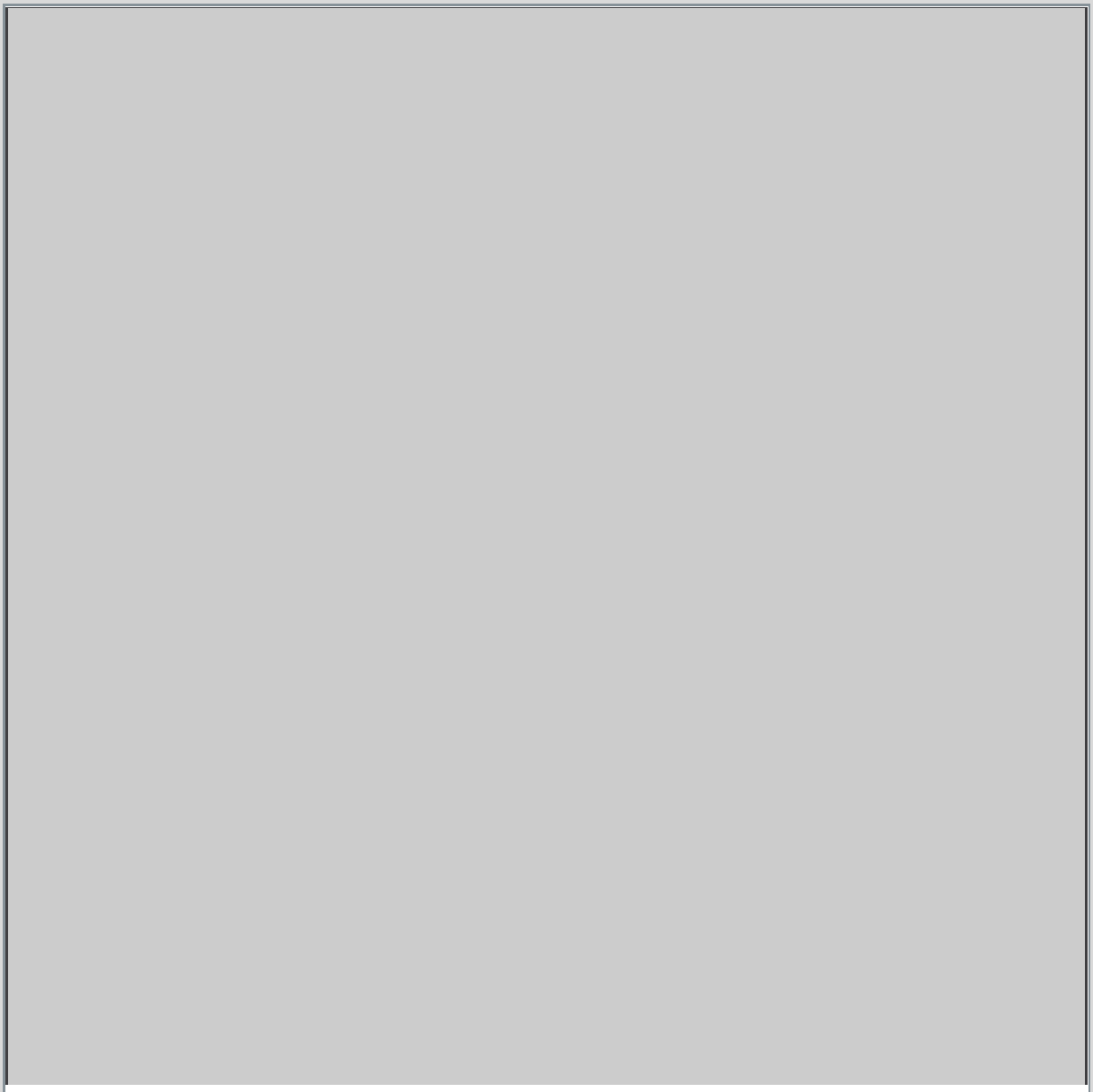
From: NW3C <training@nw3c.org>
To: james.dolehide@cookcountyil.gov, James Dolehide (Sheriff) <James.Dolehide@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:29 PM CDT
Received: June 30, 2020 11:10:31 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

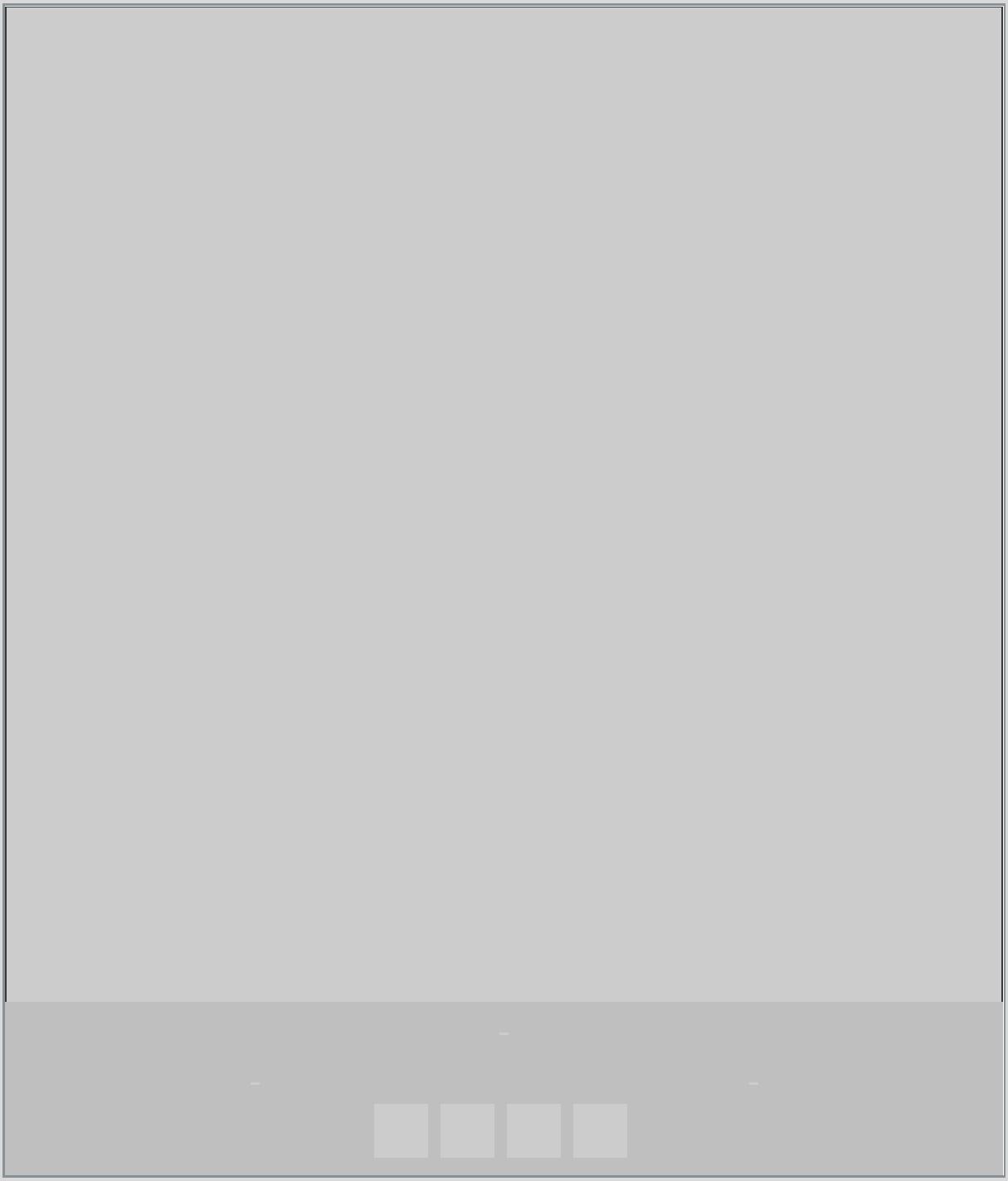
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

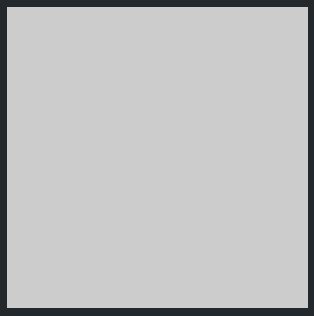
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	James Dolehide (Sheriff)
Sent:	June 30, 2020 11:10:29 PM CDT
Received:	June 30, 2020 11:10:33 PM CDT

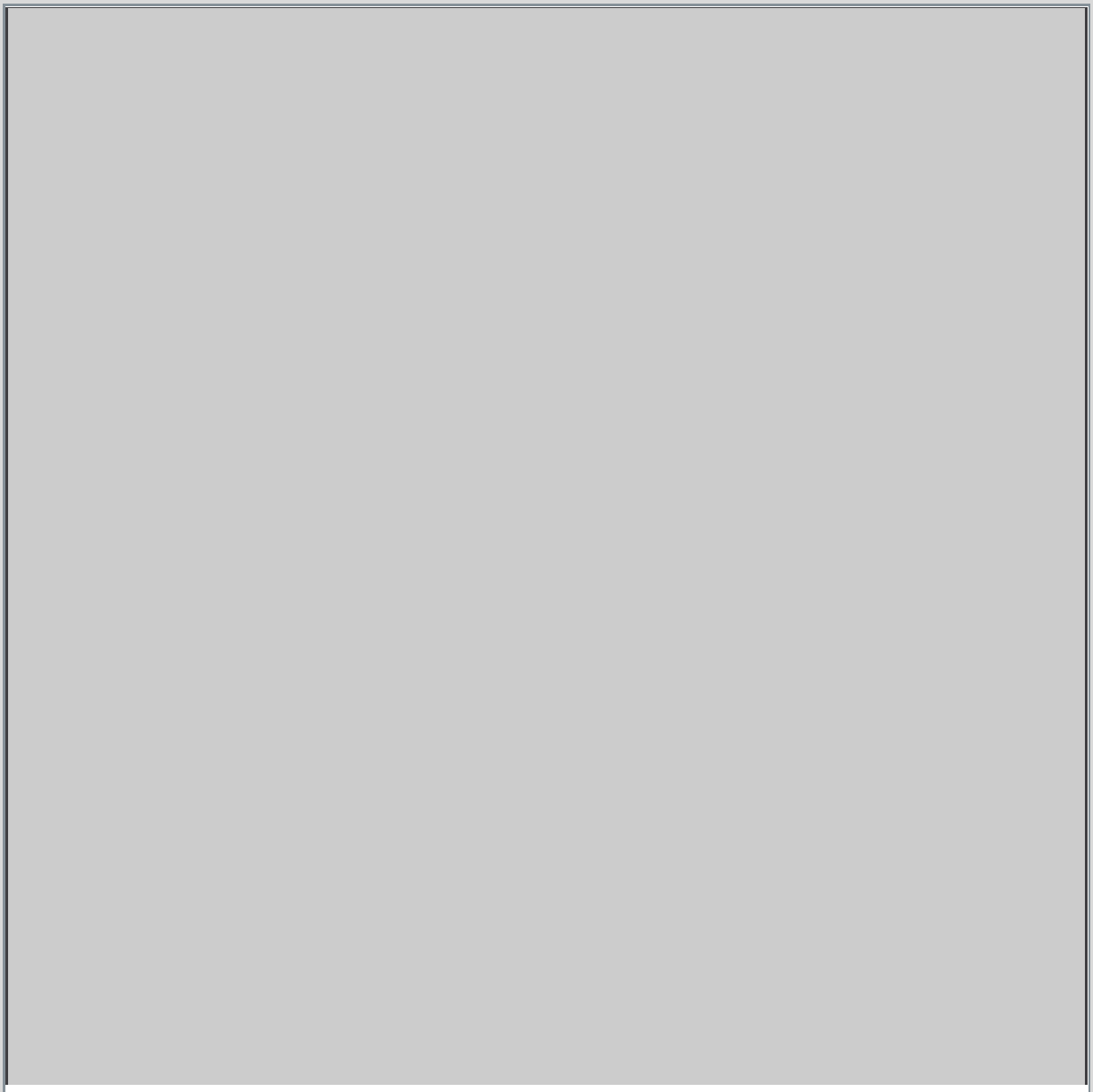
New courses available!

From:	NW3C <training@nw3c.org>
To:	ginny.georgantas@cookcountyil.gov, Ginny Georgantas (Sheriff) <Ginny.Georgantas@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:32 PM CDT
Received:	June 30, 2020 11:10:36 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

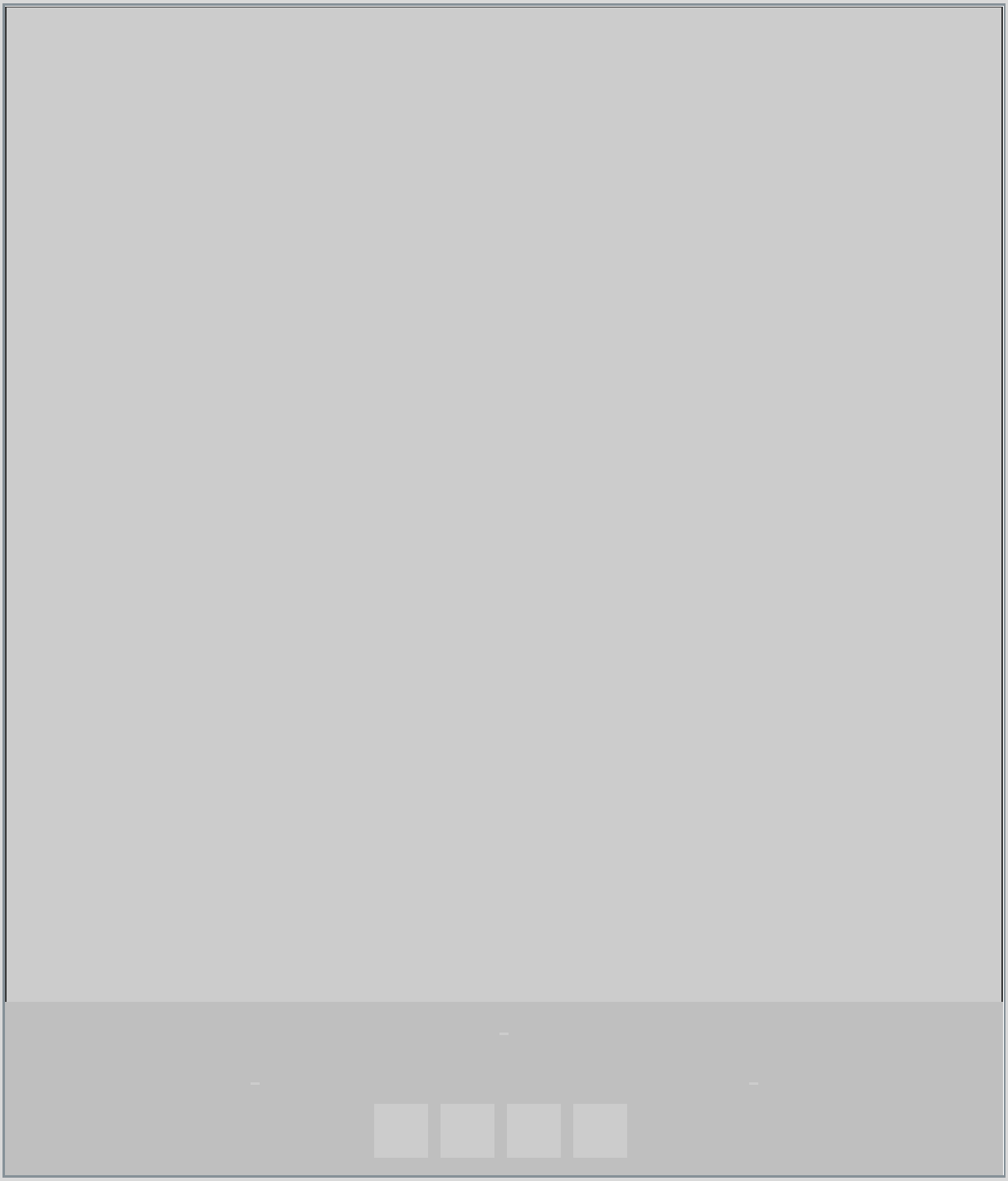
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

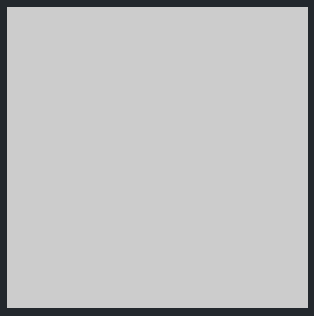
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Ginny Georgantas (Sheriff)
Sent:	June 30, 2020 11:10:32 PM CDT
Received:	June 30, 2020 11:10:37 PM CDT

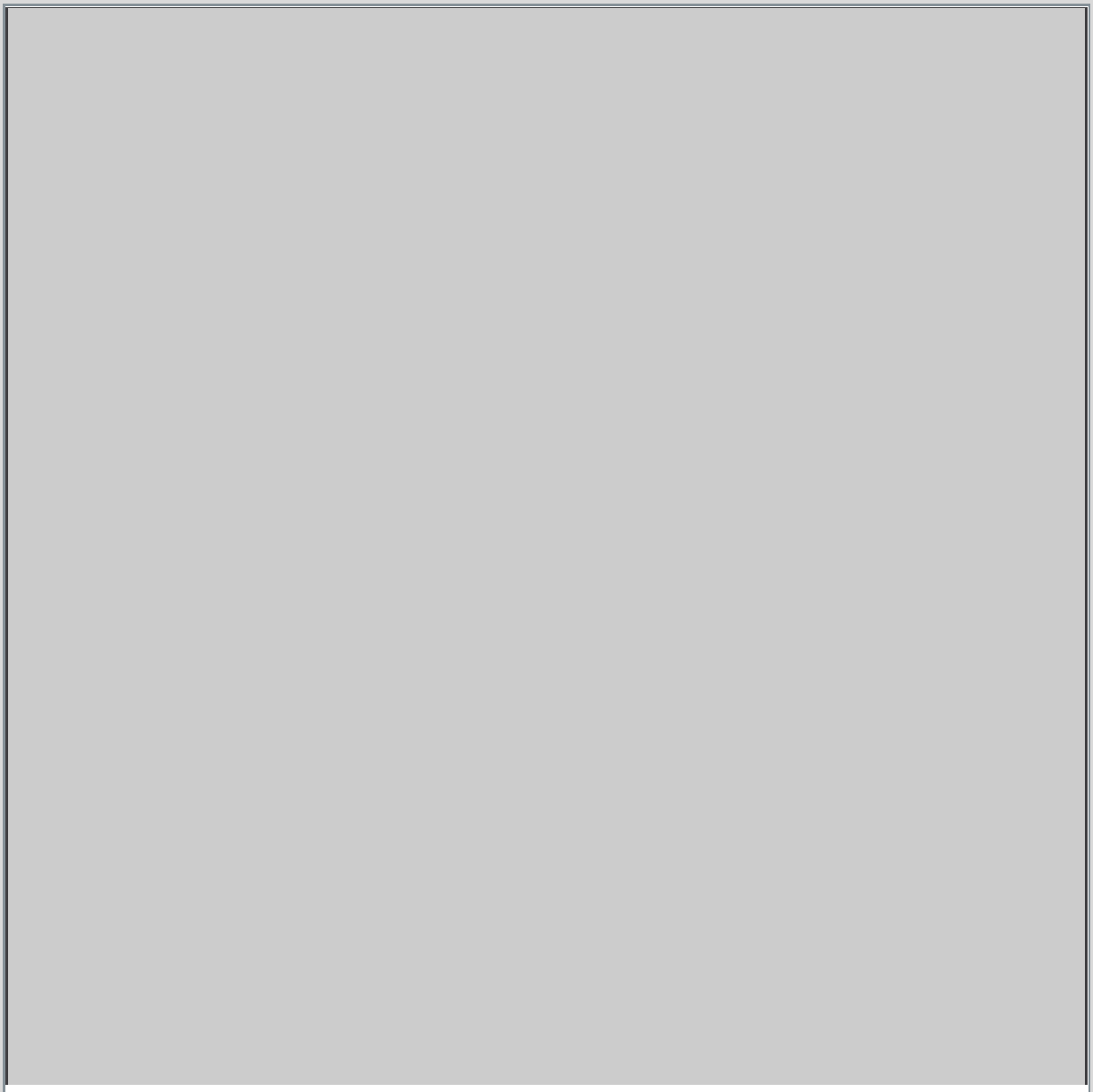
New courses available!

From:	NW3C <training@nw3c.org>
To:	christopher.dangles@cookcountyil.gov, Christopher Dangles (Sheriff) <Christopher.Dangles@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:33 PM CDT
Received:	June 30, 2020 11:10:34 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

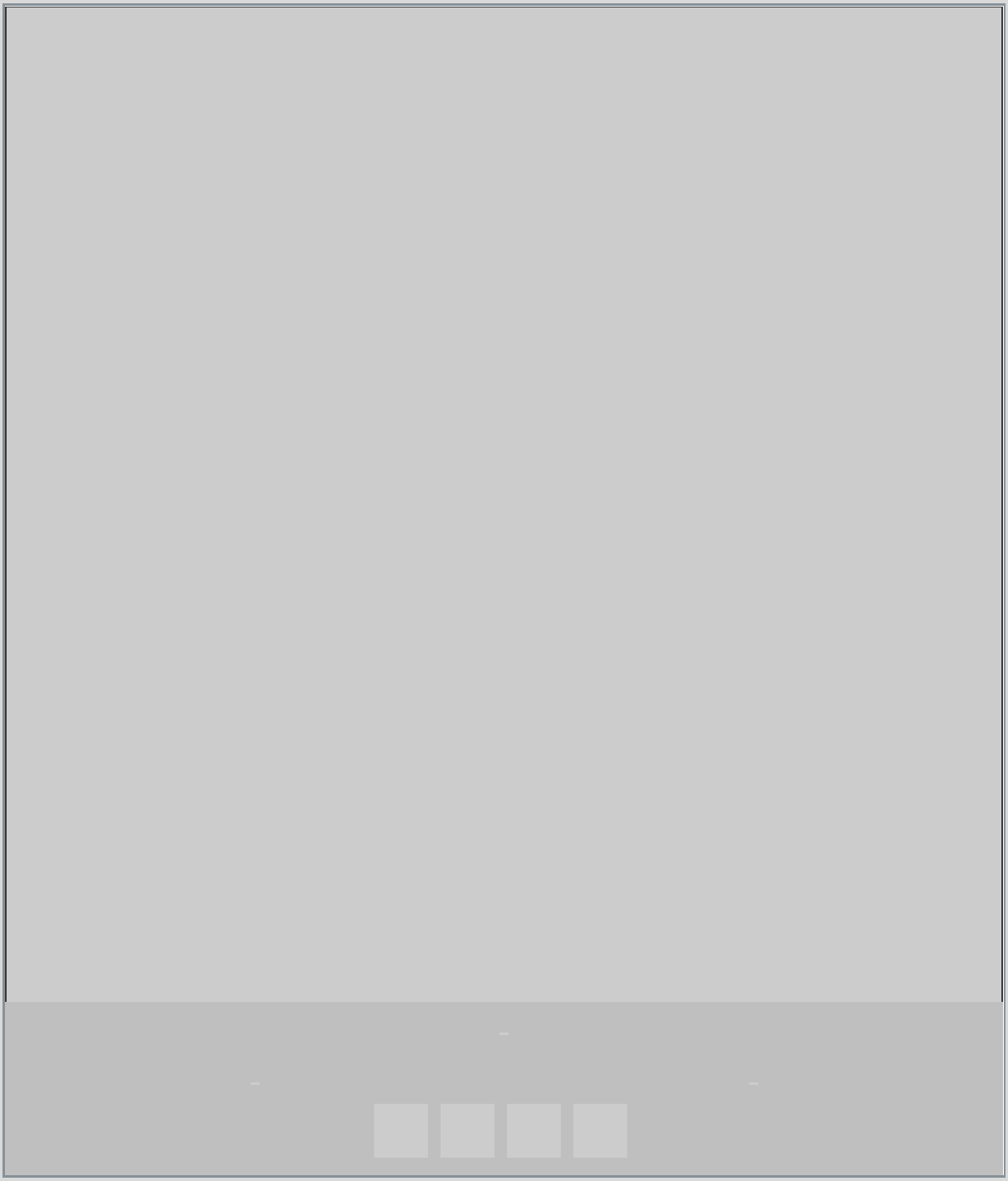
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

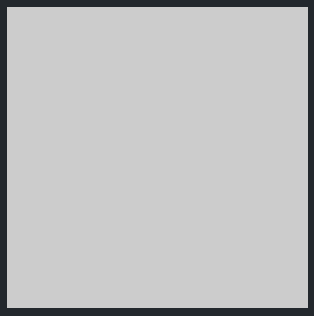
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Christopher Dangles (Sheriff)
Sent:	June 30, 2020 11:10:33 PM CDT
Received:	June 30, 2020 11:10:35 PM CDT

New courses available!

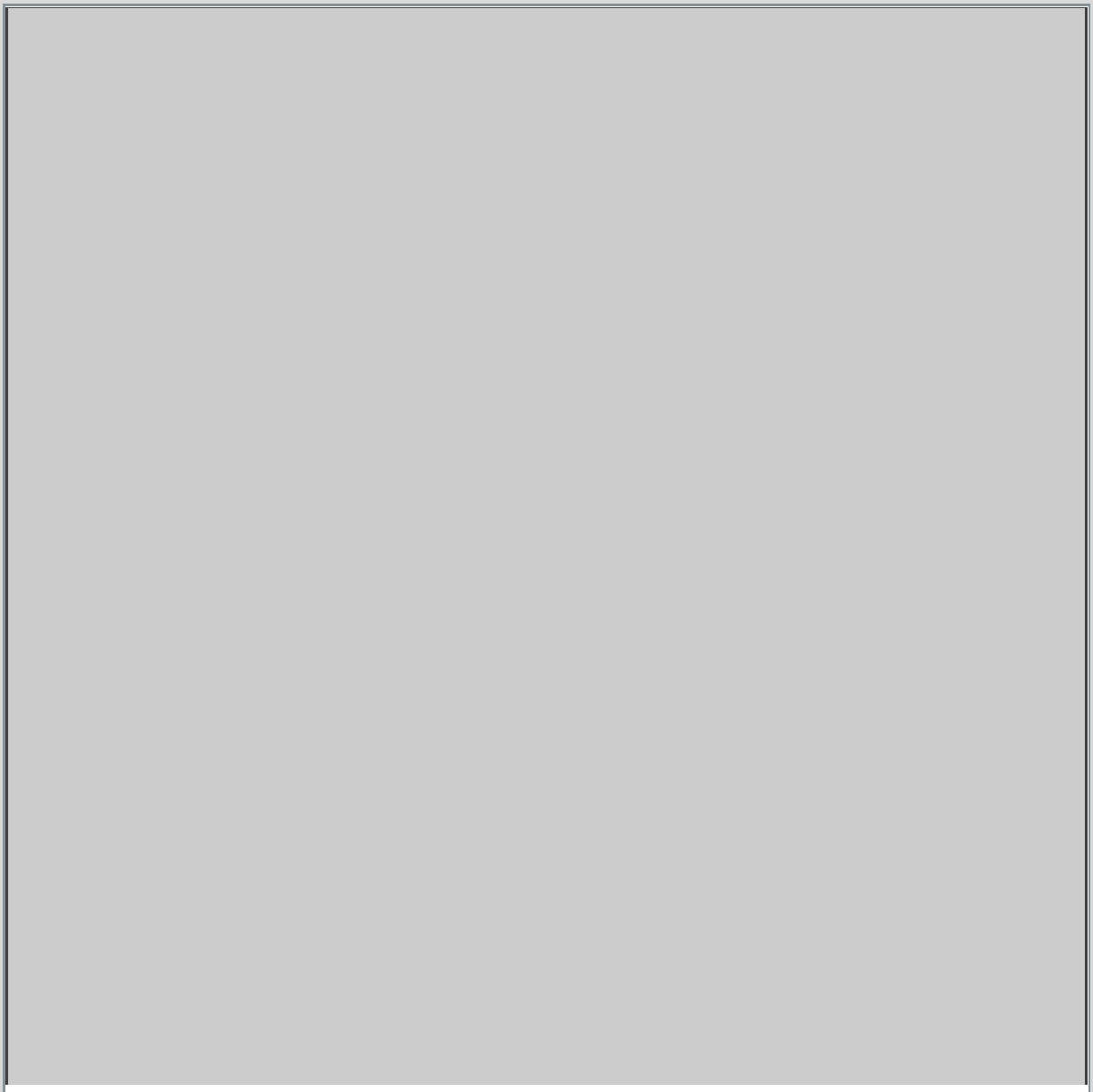
From: NW3C <training@nw3c.org>
To: michael.dwyer@cookcountyil.gov, Michael Dwyer (Sheriff) <Michael.Dwyer@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:39 PM CDT
Received: June 30, 2020 11:10:42 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

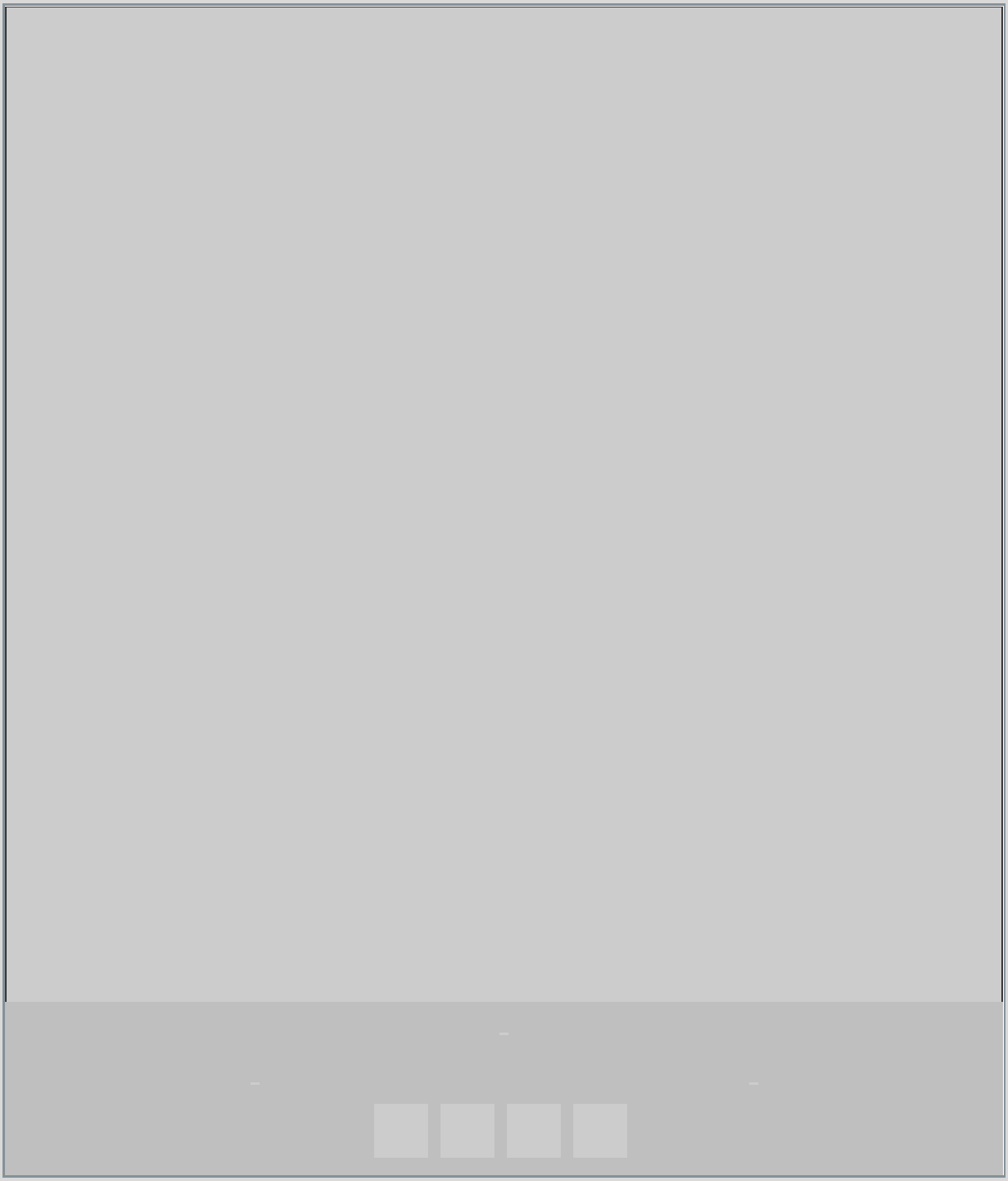
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

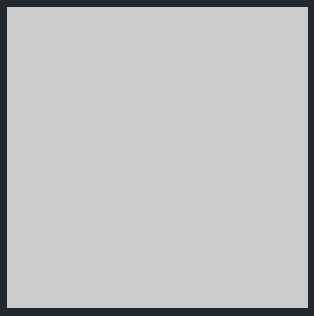
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

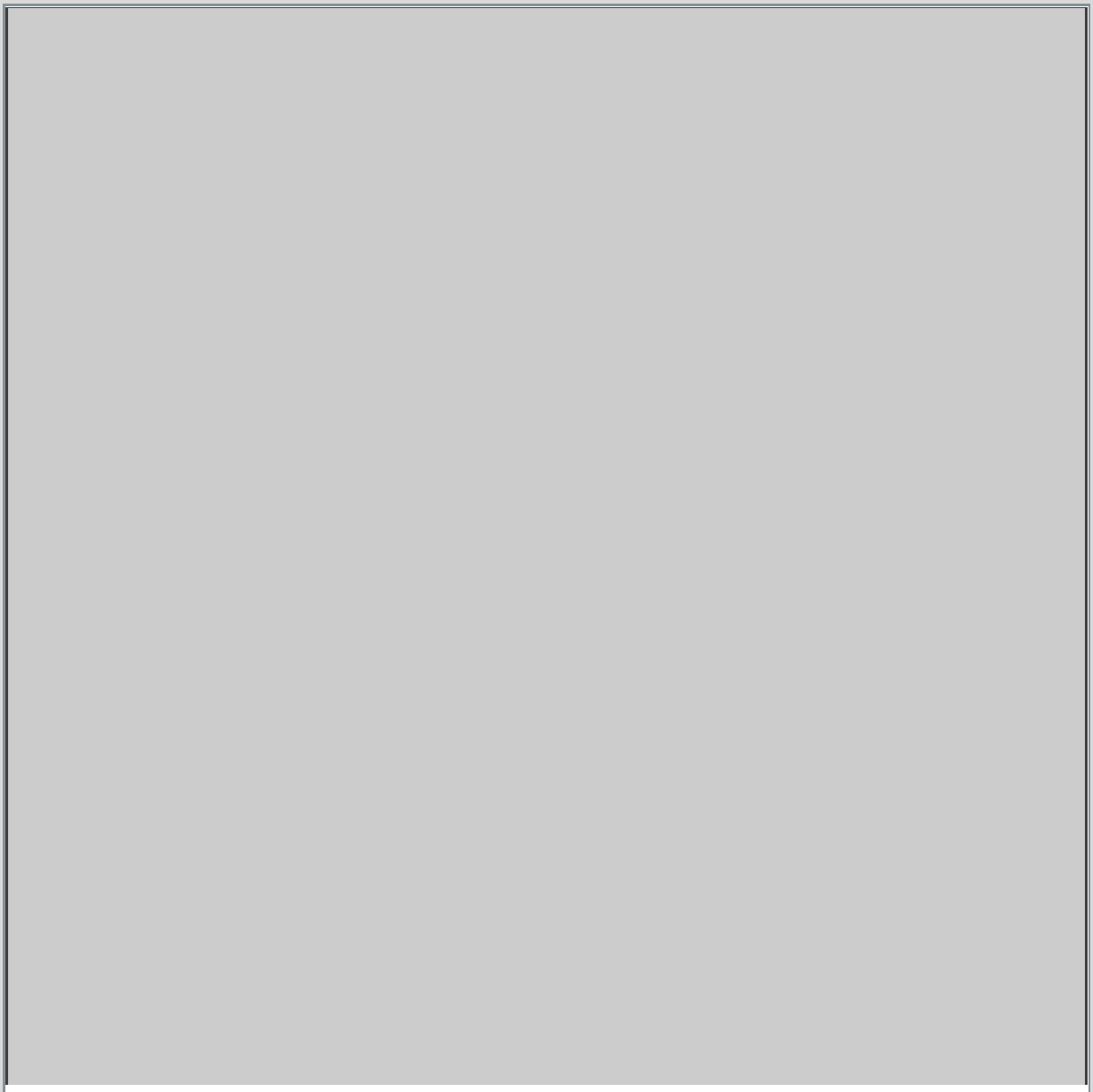
From: NW3C <training@nw3c.org>
To: robert.hausherr@cookcountyil.gov, Robert Hausherr (Sheriff) <Robert.Hausherr@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:40 PM CDT
Received: June 30, 2020 11:10:42 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

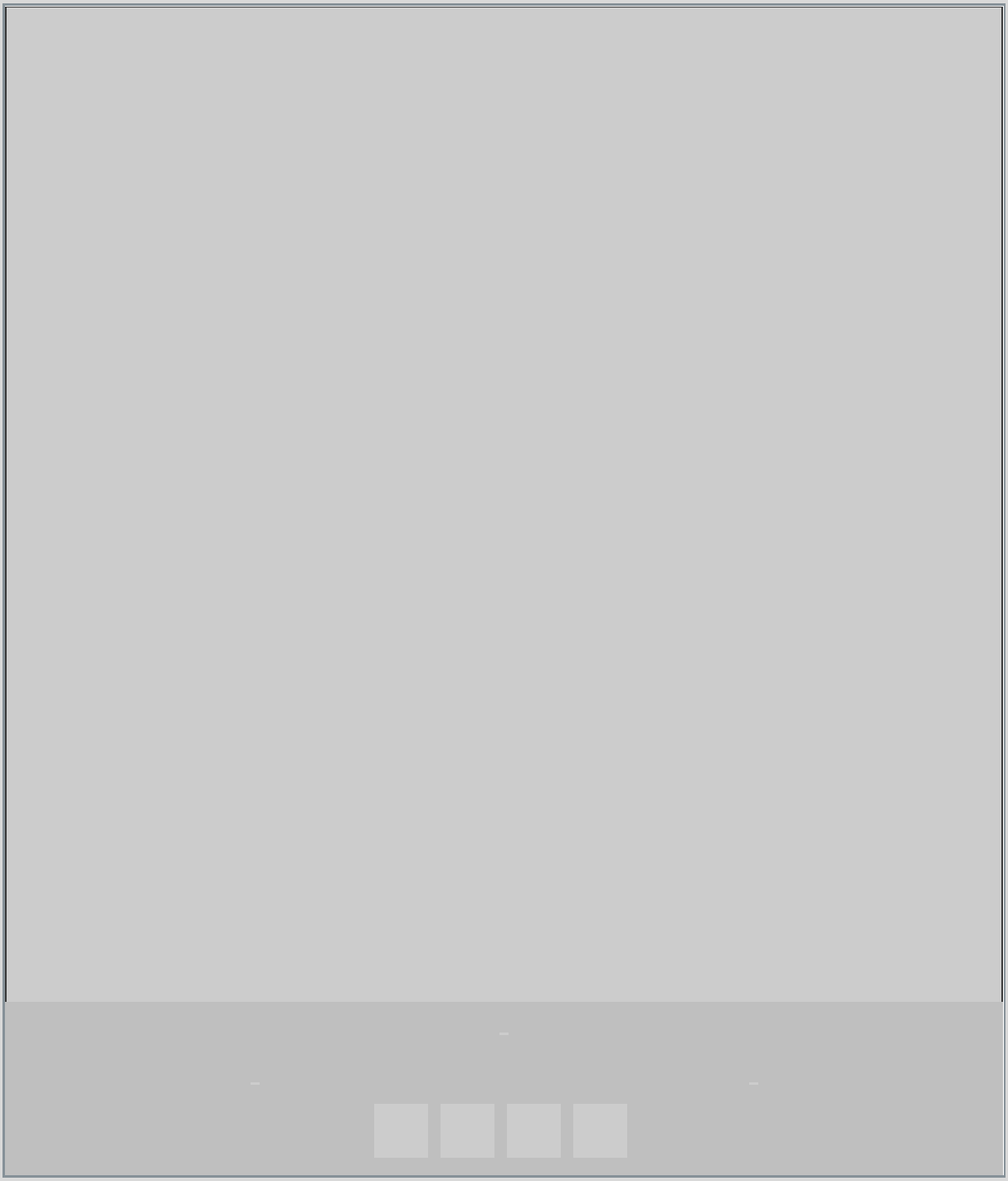
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

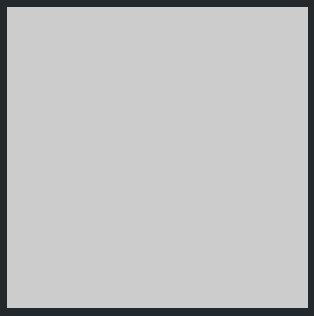
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Robert Hausherr (Sheriff)
Sent:	June 30, 2020 11:10:40 PM CDT
Received:	June 30, 2020 11:10:43 PM CDT

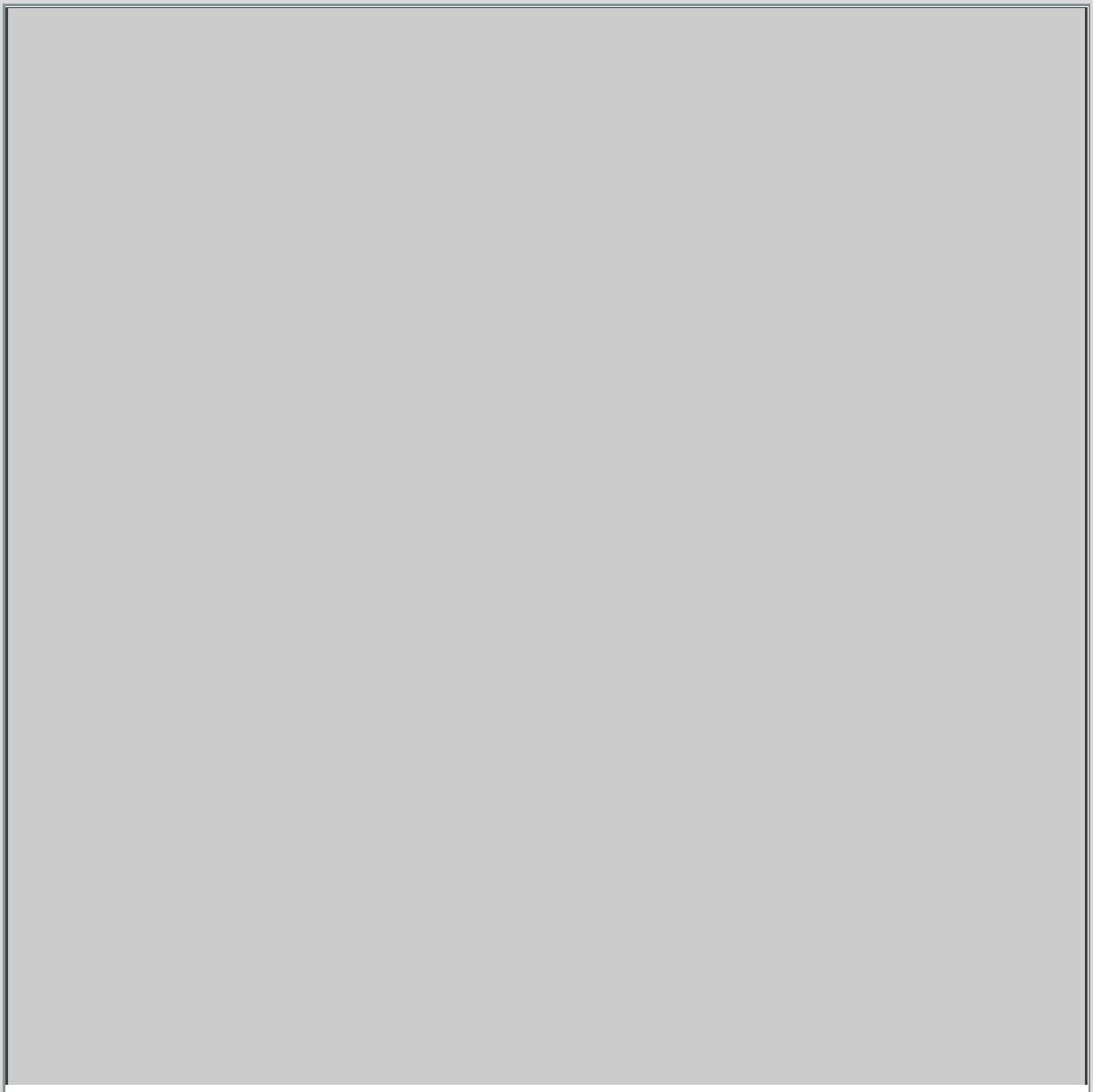
New courses available!

From:	NW3C <training@nw3c.org>
To:	krzysztof.wantuch@cookcountyil.gov, Krzysztof Wantuch (Sheriff) <Krzysztof.Wantuch@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:41 PM CDT
Received:	June 30, 2020 11:10:43 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

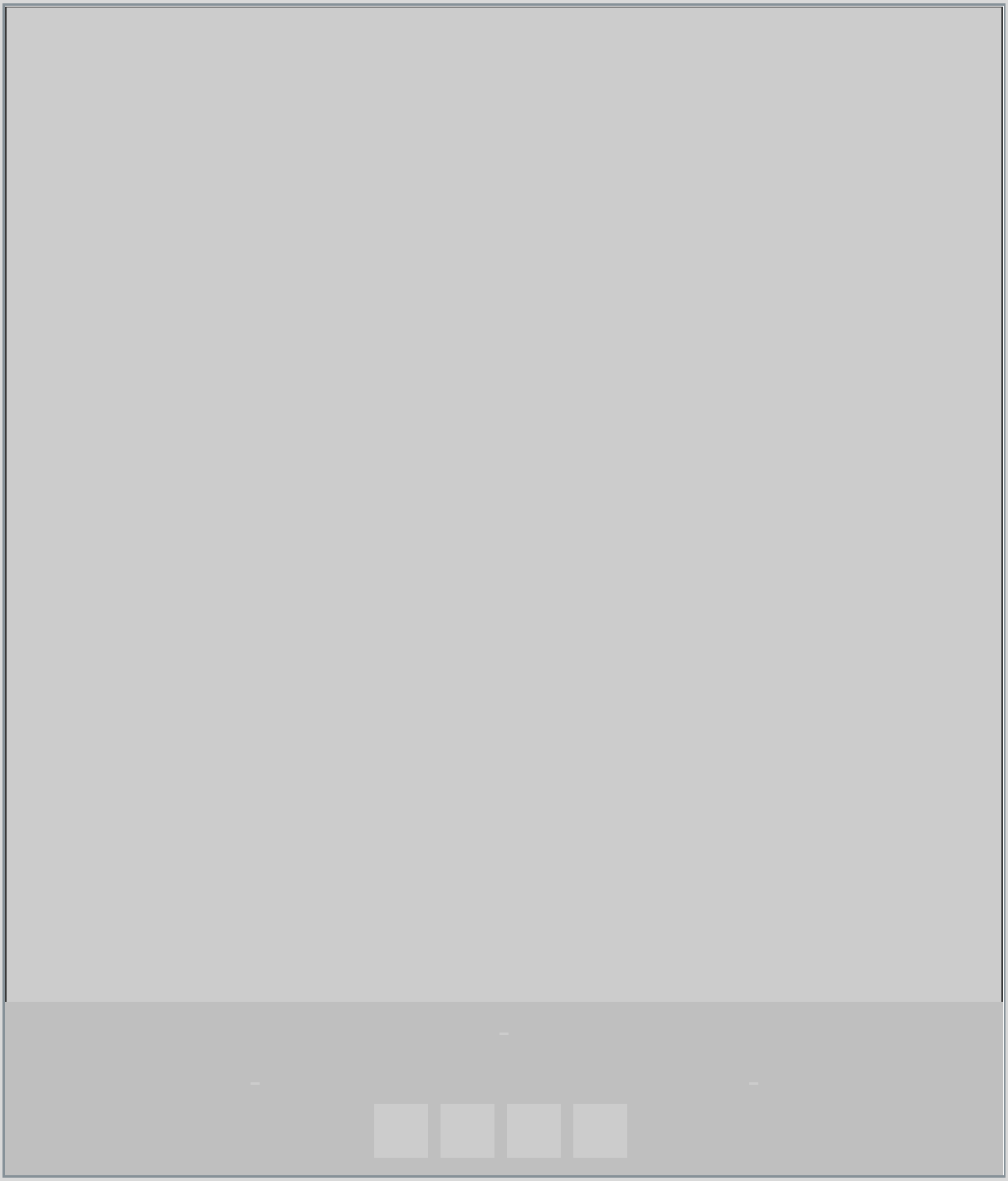
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

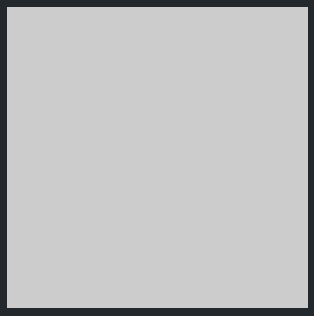
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Krzysztof Wantuch (Sheriff)
Sent:	June 30, 2020 11:10:41 PM CDT
Received:	June 30, 2020 11:10:44 PM CDT

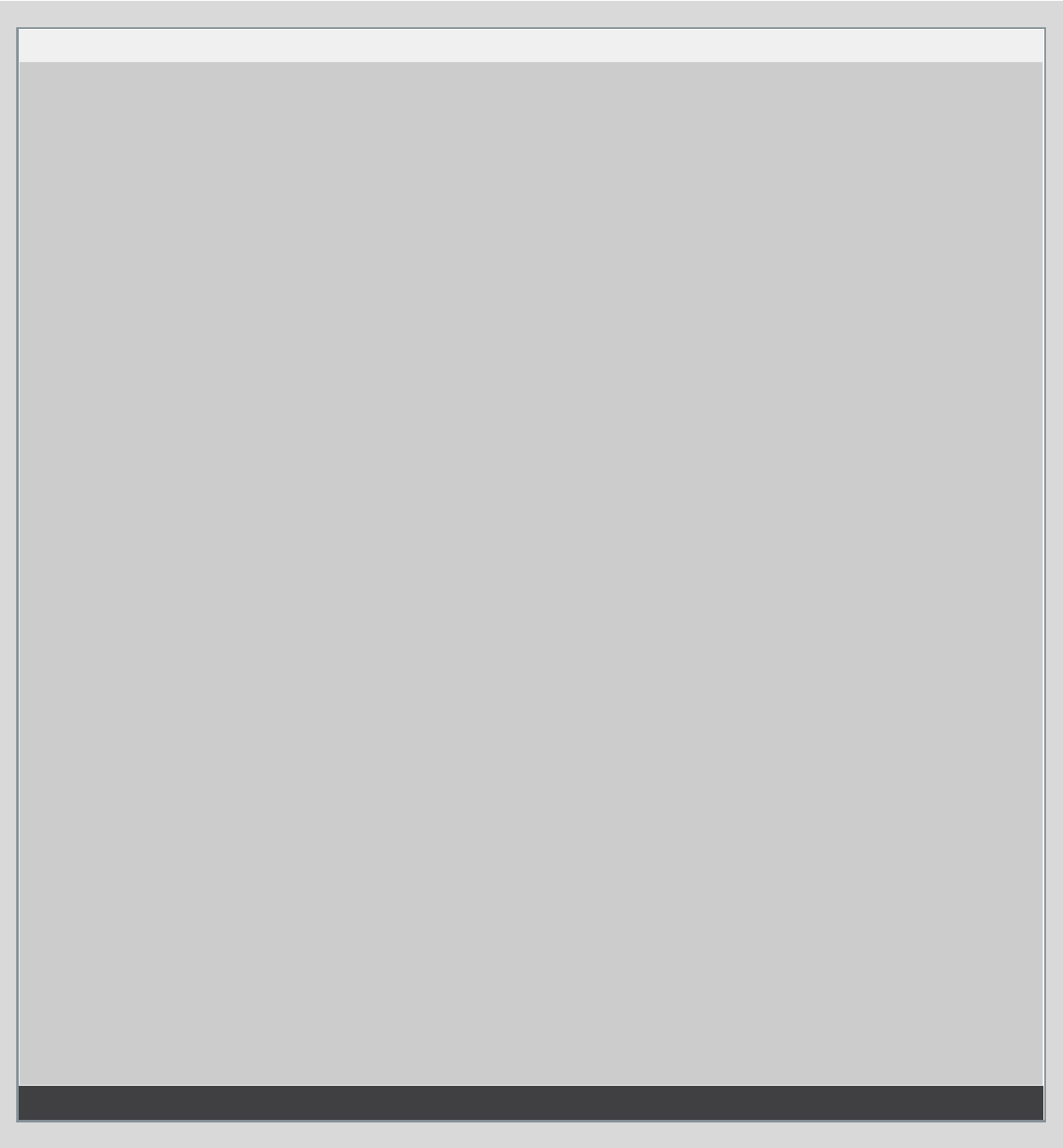
New courses available!

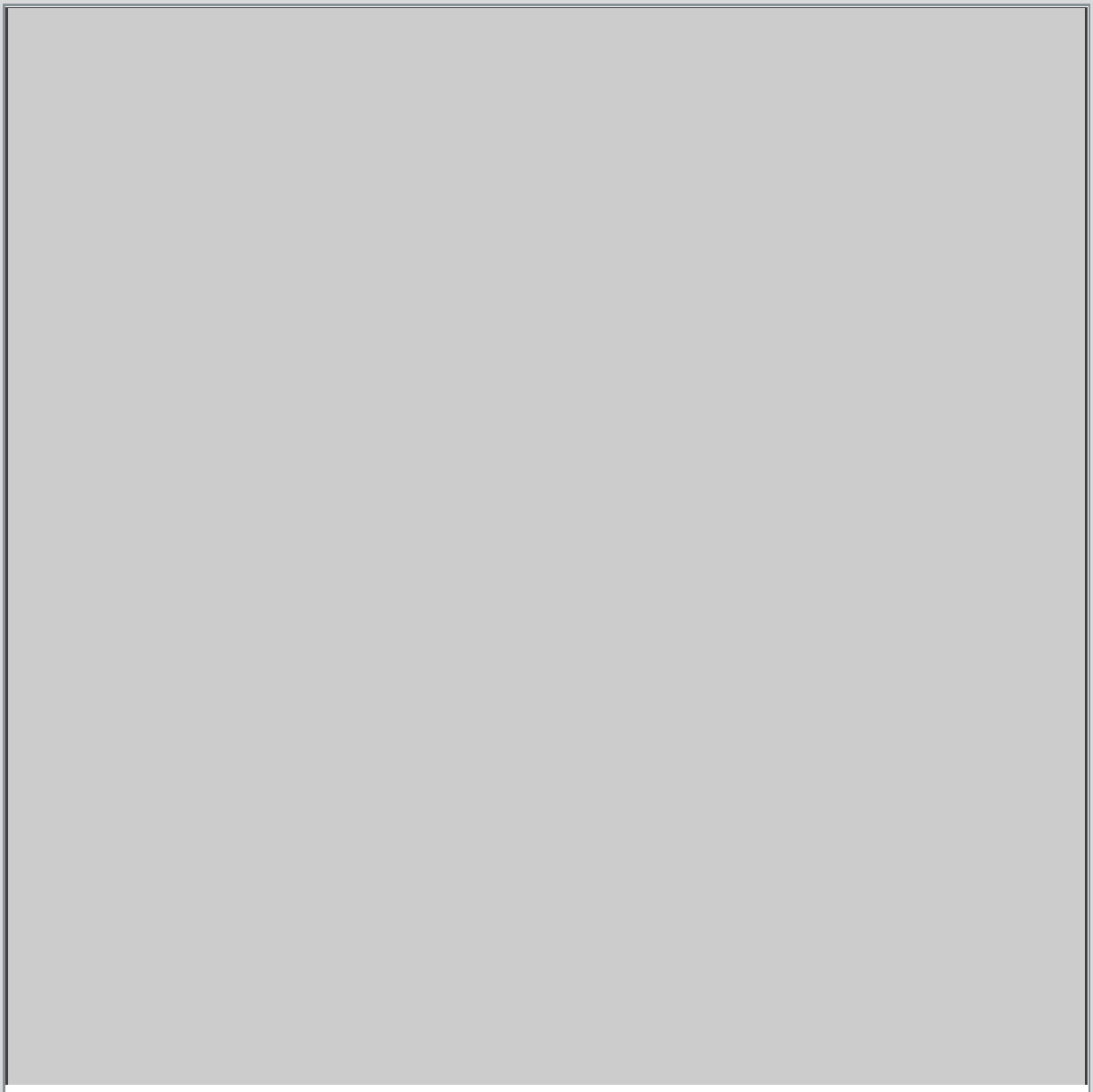
From: NW3C <training@nw3c.org>
To: devlin.gray@cookcountyil.gov, Devlin Gray (Sheriff) <Devlin.Gray@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:42 PM CDT
Received: June 30, 2020 11:10:44 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

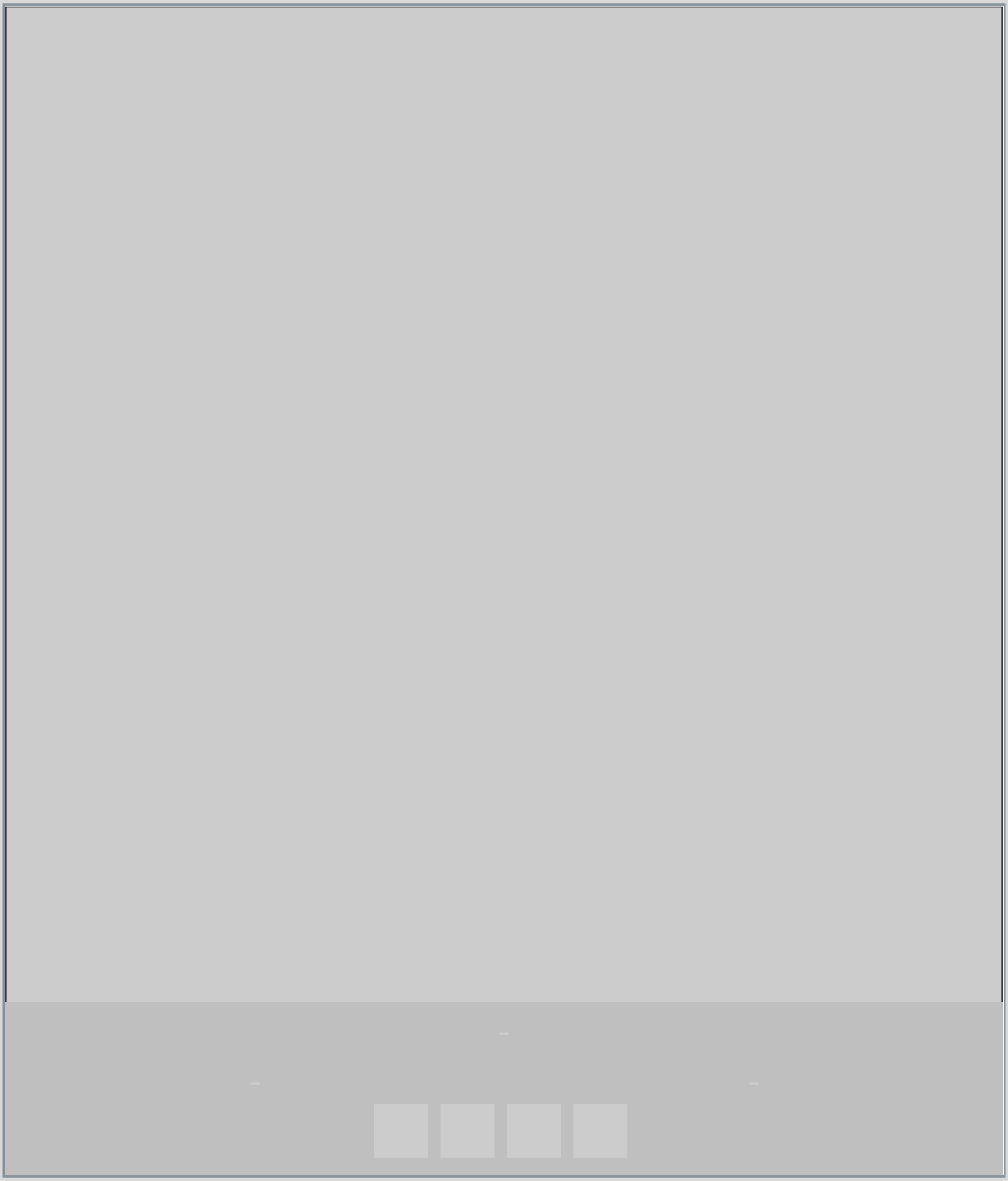
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

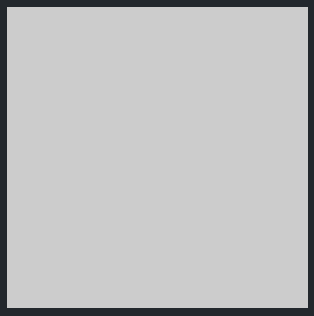
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

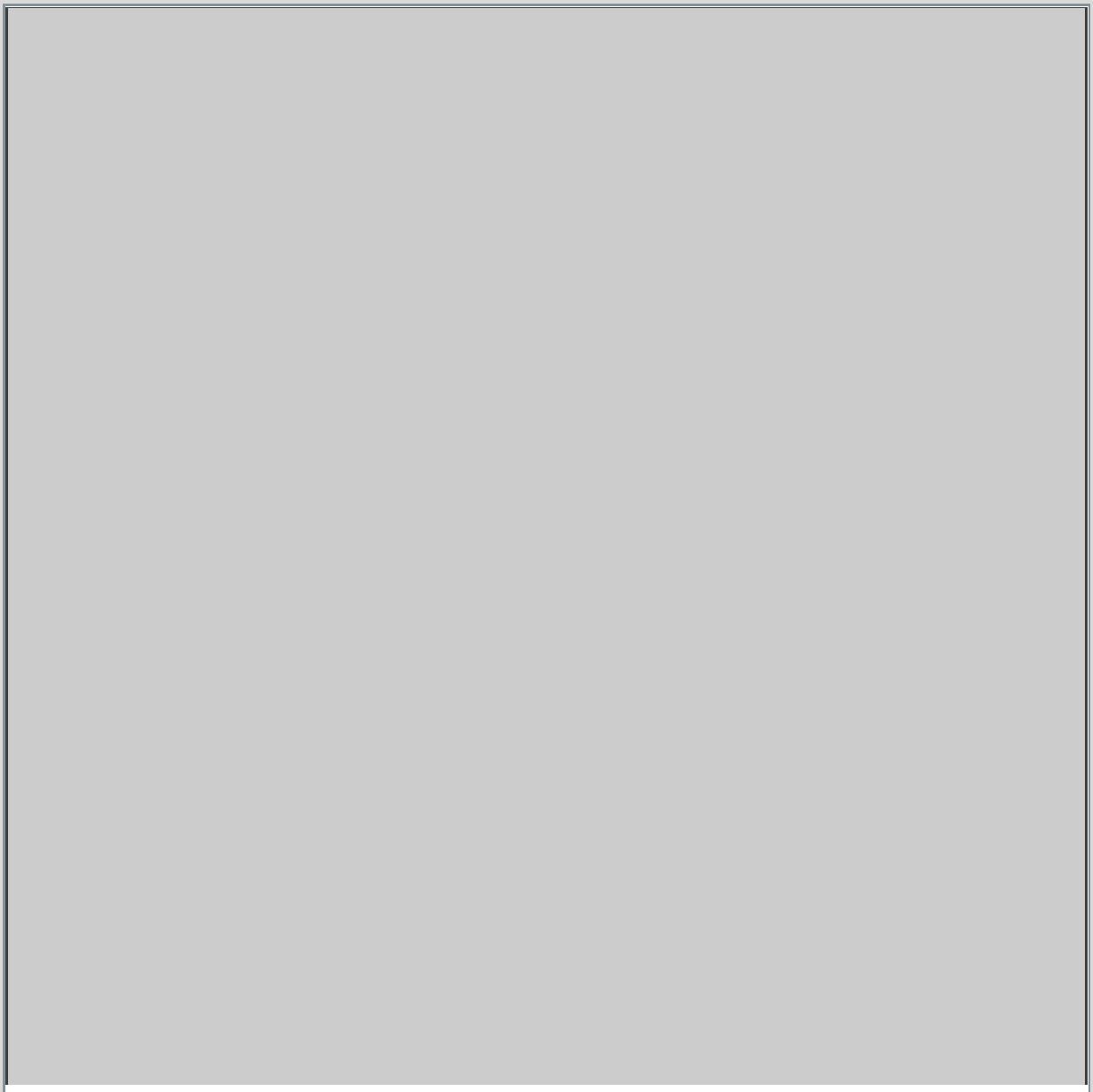
New courses available!

From:	NW3C <training@nw3c.org>
To:	steven.zepeda@cookcountyil.gov, Steven Zepeda (Sheriff) <Steven.Zepeda@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:42 PM CDT
Received:	June 30, 2020 11:10:46 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

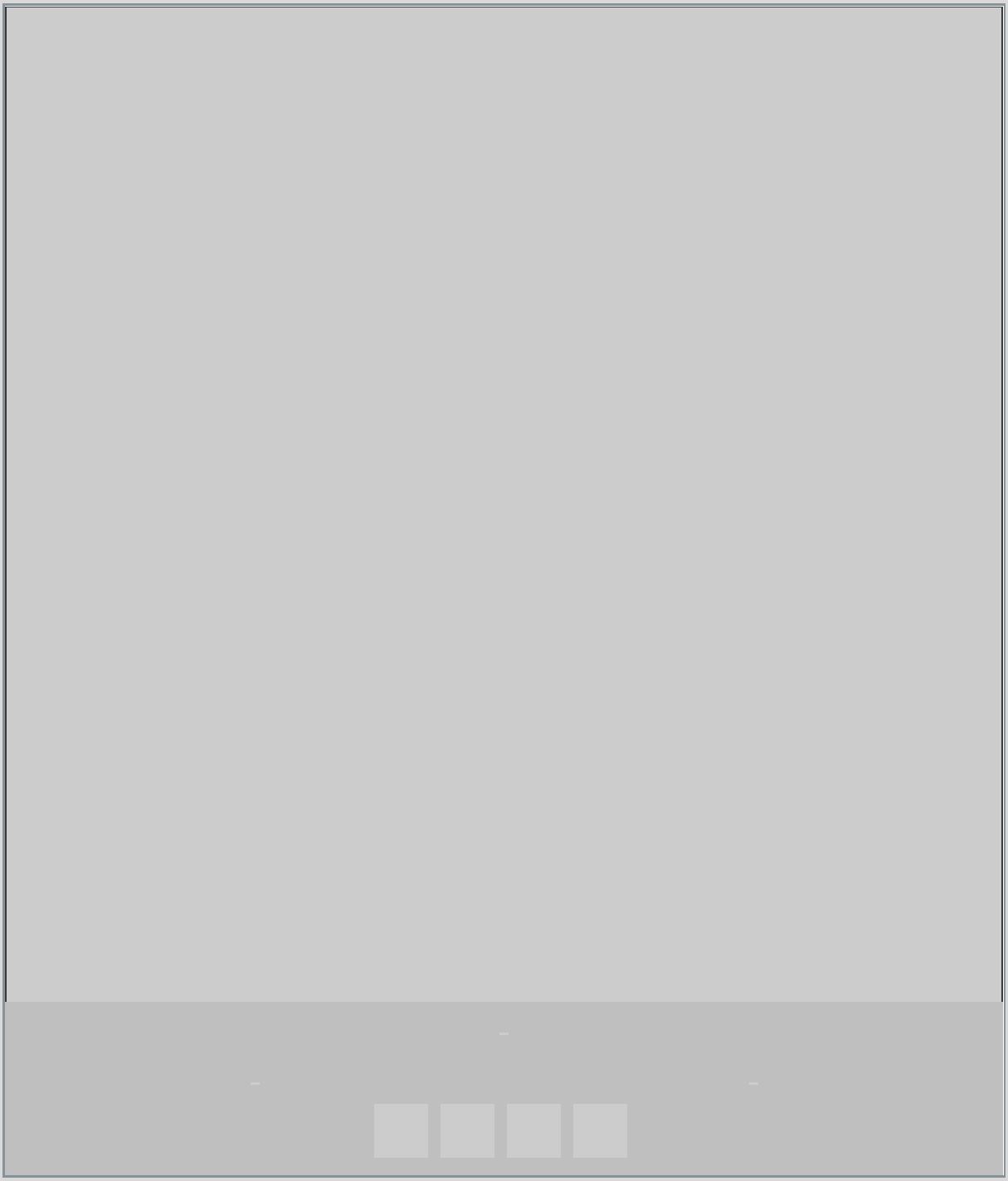
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

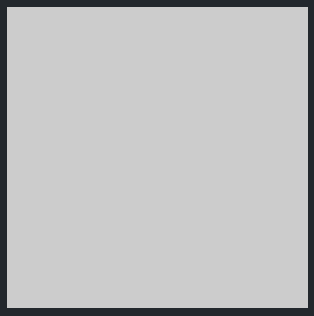
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

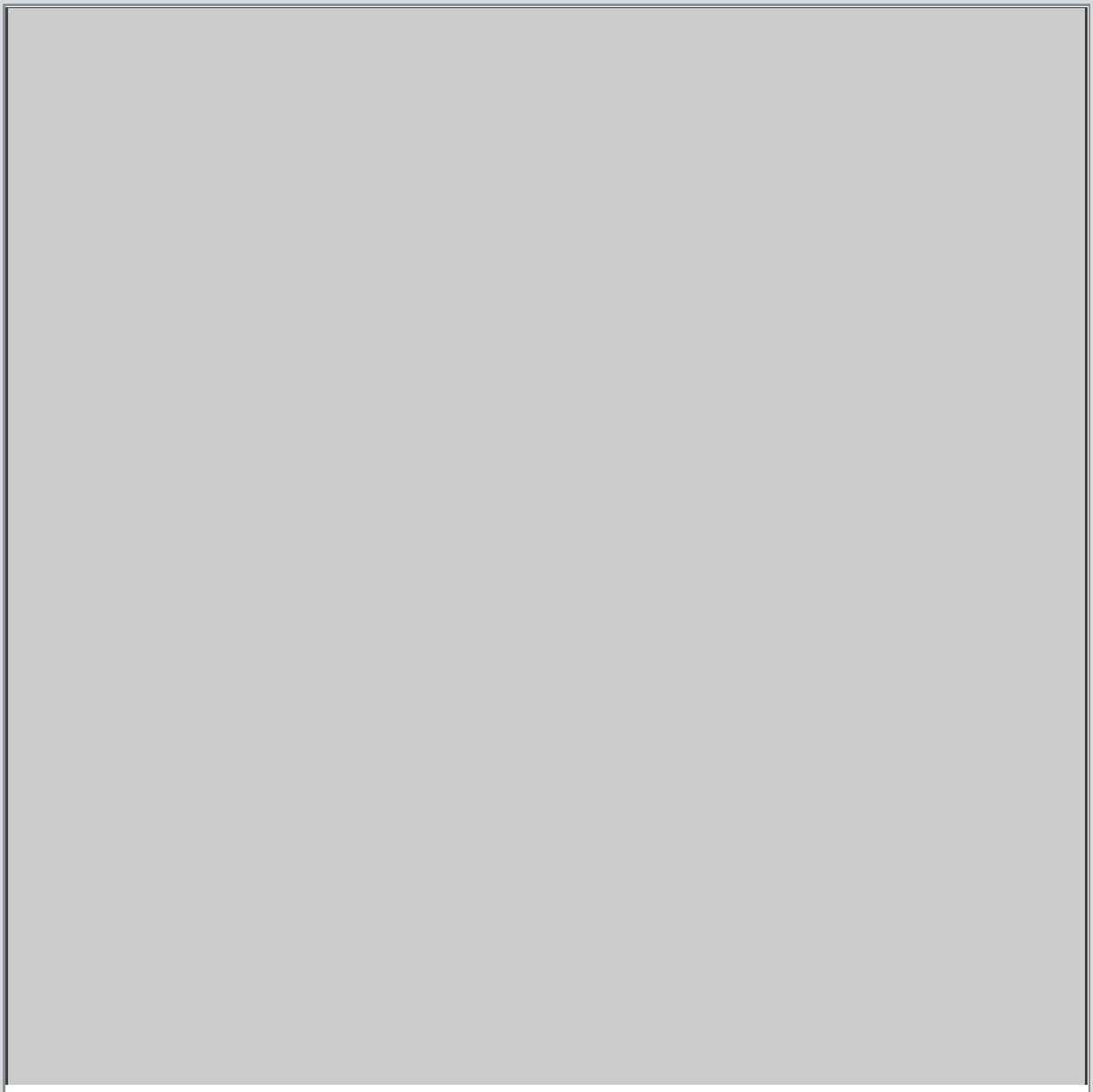
From: NW3C <training@nw3c.org>
To: richard.garcia2@cookcountyil.gov, Richard Garcia (Sheriff) <Richard.Garcia2@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:42 PM CDT
Received: June 30, 2020 11:10:45 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

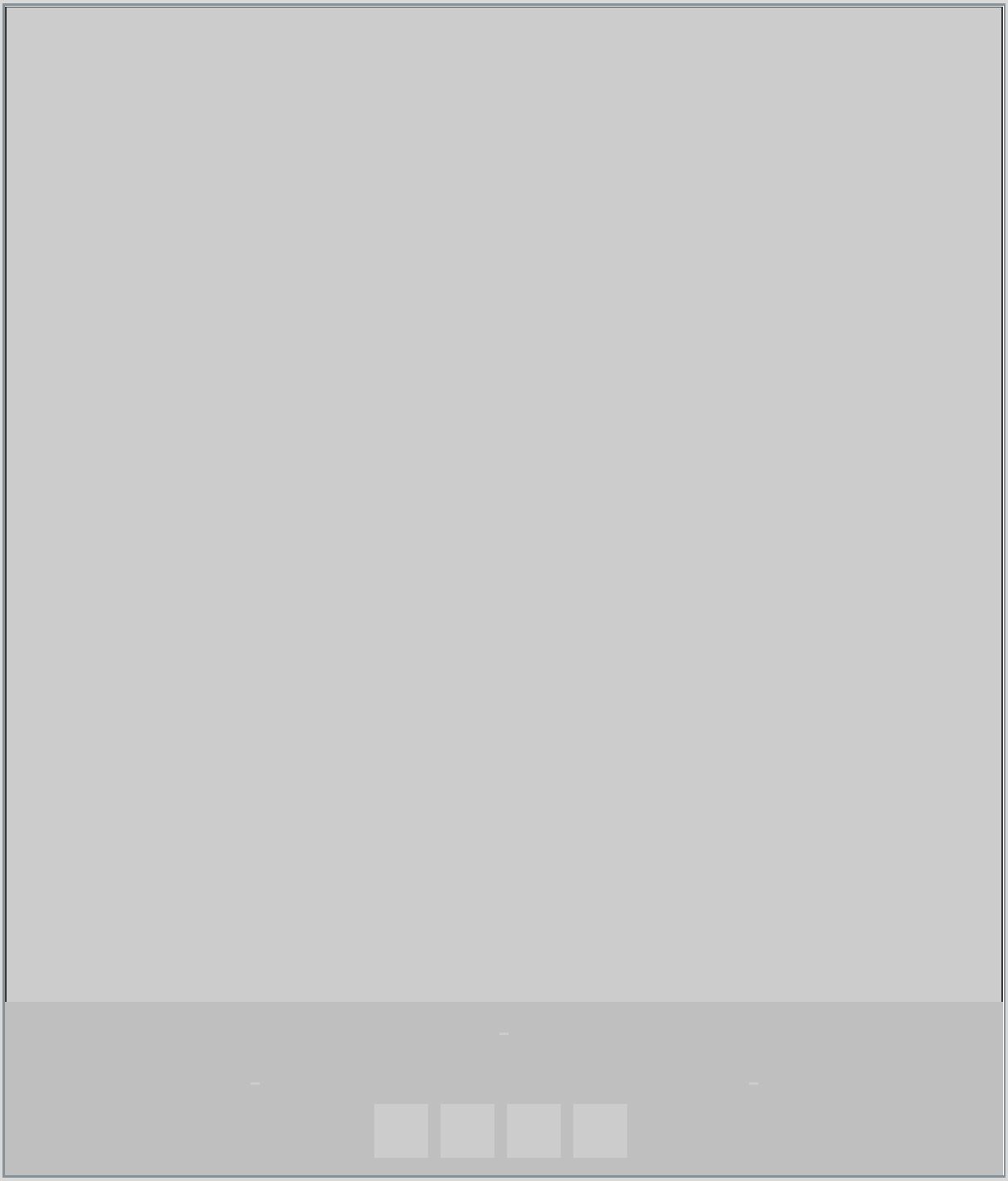
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

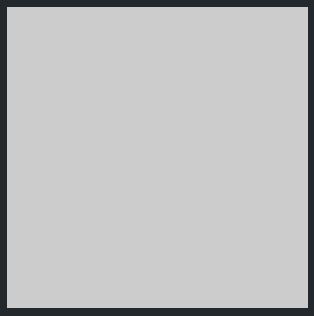
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Devlin Gray (Sheriff)
Sent:	June 30, 2020 11:10:42 PM CDT
Received:	June 30, 2020 11:10:45 PM CDT

New courses available!

To:	Steven Zepeda (Sheriff)
Sent:	June 30, 2020 11:10:42 PM CDT
Received:	June 30, 2020 11:10:46 PM CDT

New courses available!

To:	Richard Garcia (Sheriff)
Sent:	June 30, 2020 11:10:42 PM CDT
Received:	June 30, 2020 11:10:45 PM CDT

New courses available!

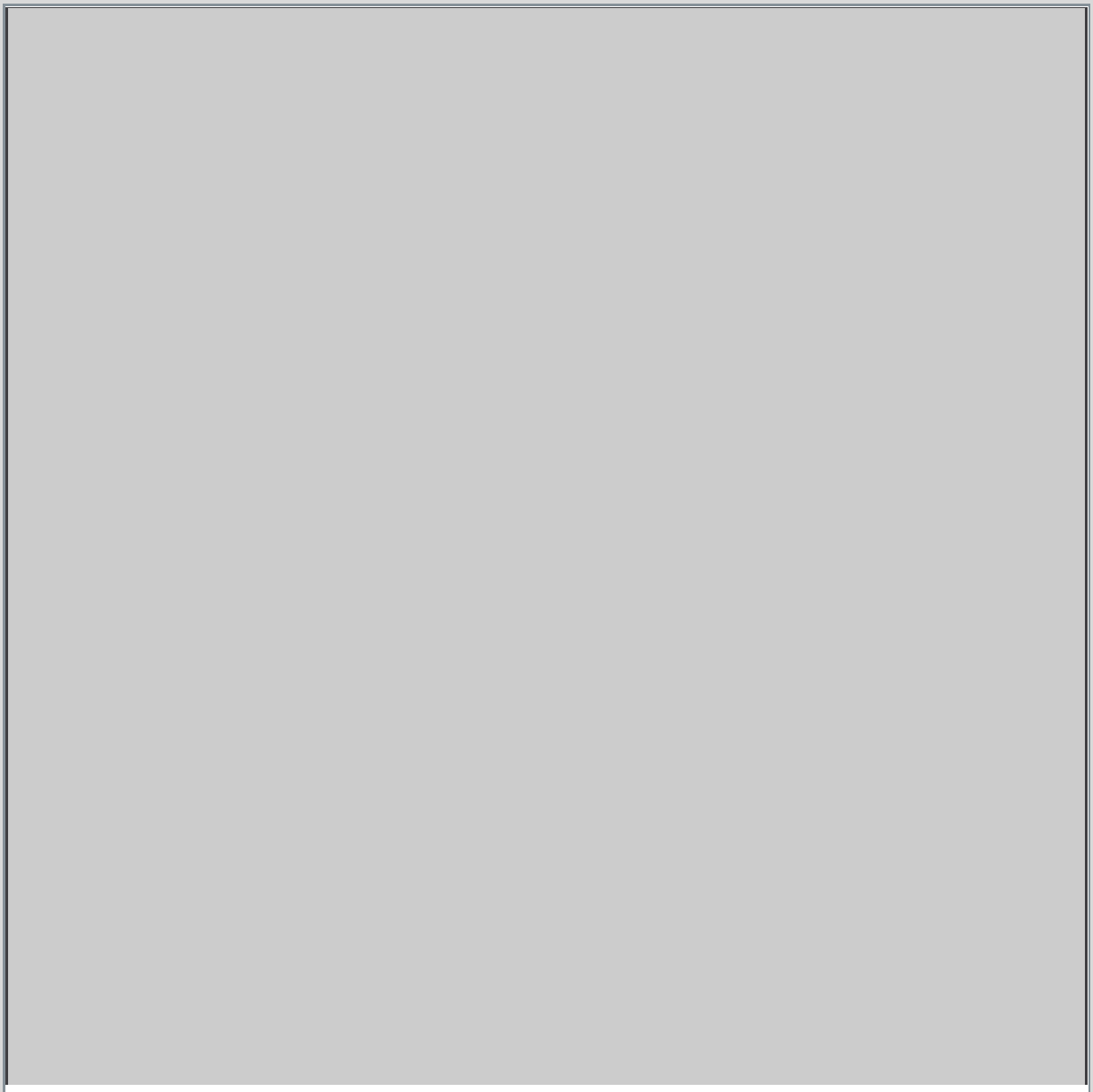
From: NW3C <training@nw3c.org>
To: henry.hemphill@cookcountyil.gov, Henry Hemphill (Sheriff) <Henry.Hemphill@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:45 PM CDT
Received: June 30, 2020 11:10:47 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

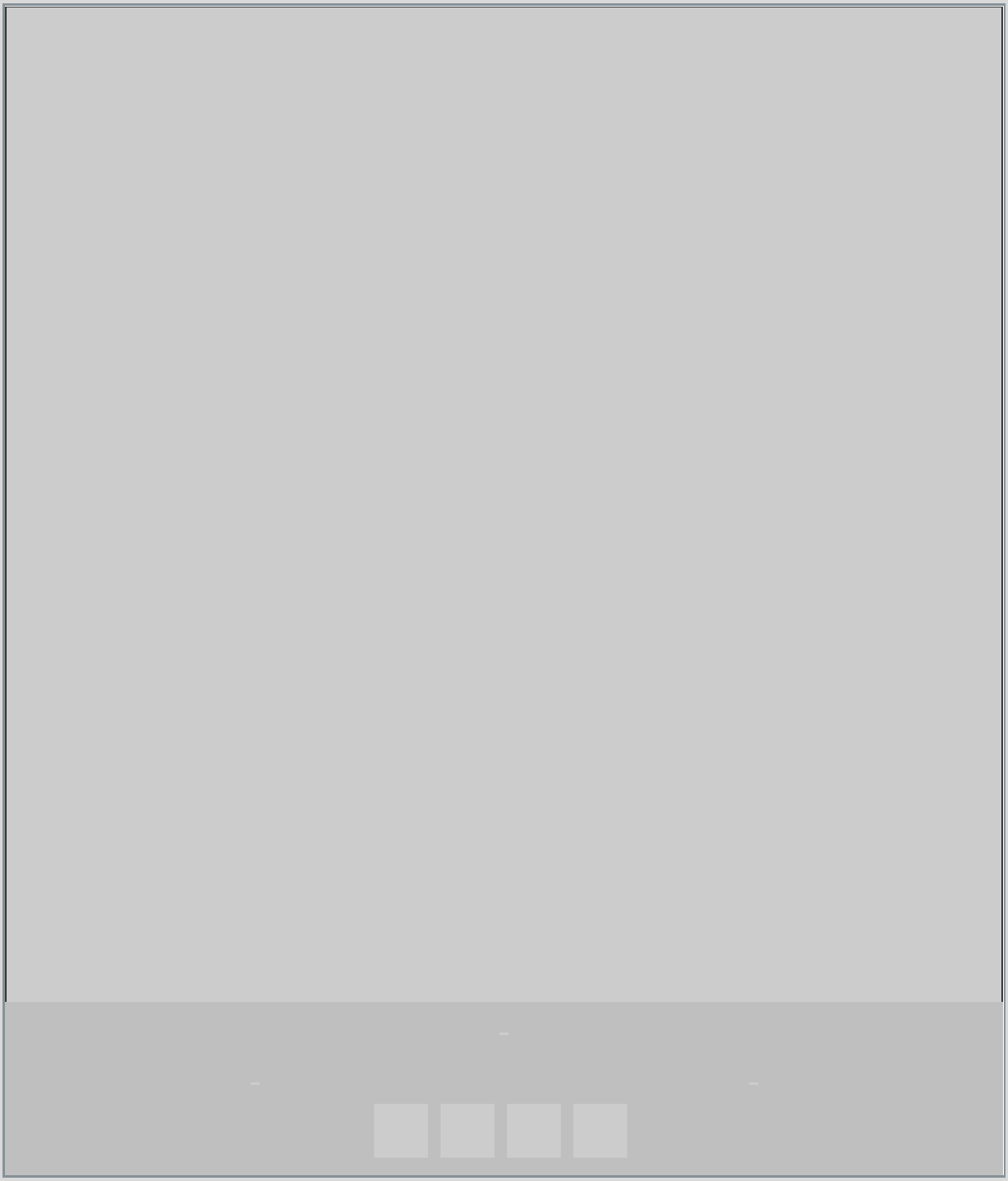
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

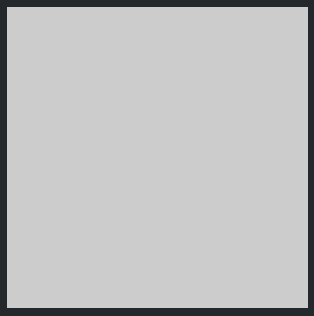
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Henry Hemphill (Sheriff)
Sent:	June 30, 2020 11:10:45 PM CDT
Received:	June 30, 2020 11:10:48 PM CDT

New courses available!

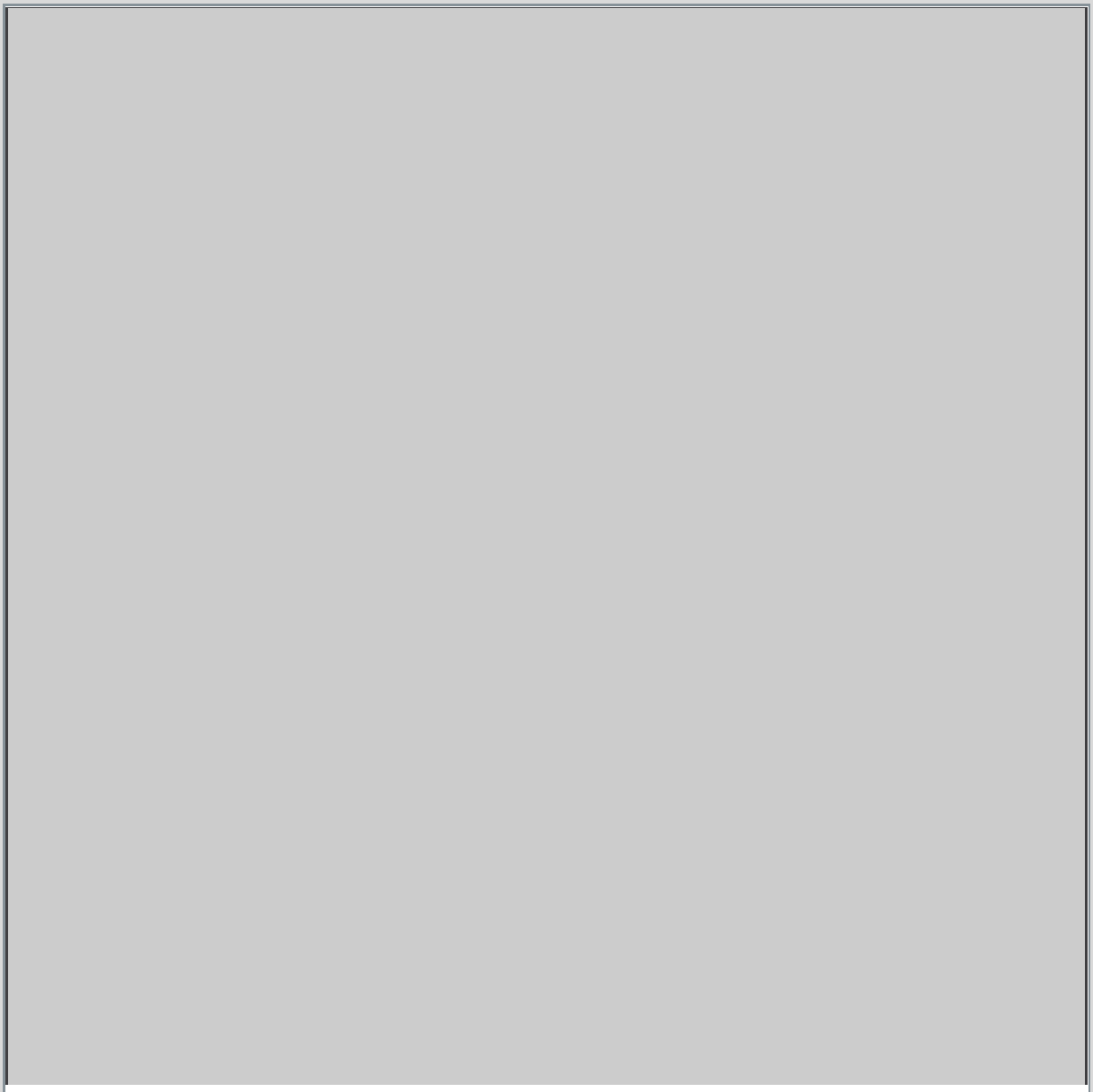
From: NW3C <training@nw3c.org>
To: michael.kizaric@cookcountyil.gov, Michael Kizaric (Sheriff) <Michael.Kizaric@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:46 PM CDT
Received: June 30, 2020 11:10:48 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

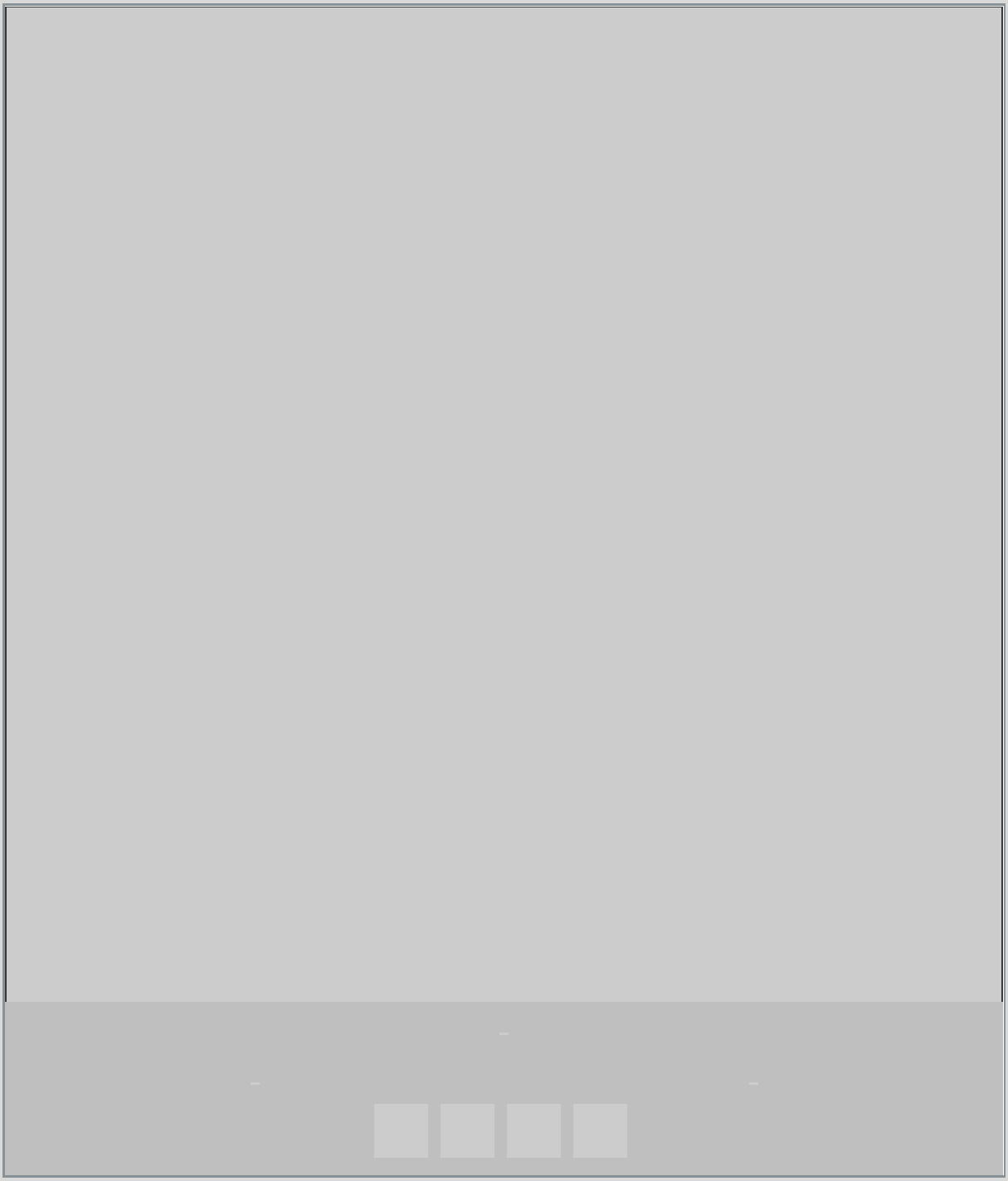
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

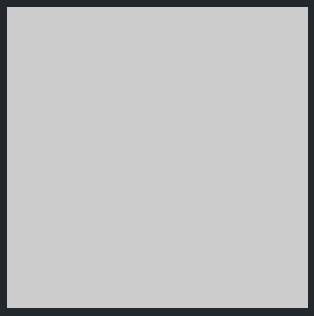
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Michael Kizaric (Sheriff)
Sent:	June 30, 2020 11:10:46 PM CDT
Received:	June 30, 2020 11:10:49 PM CDT

New courses available!

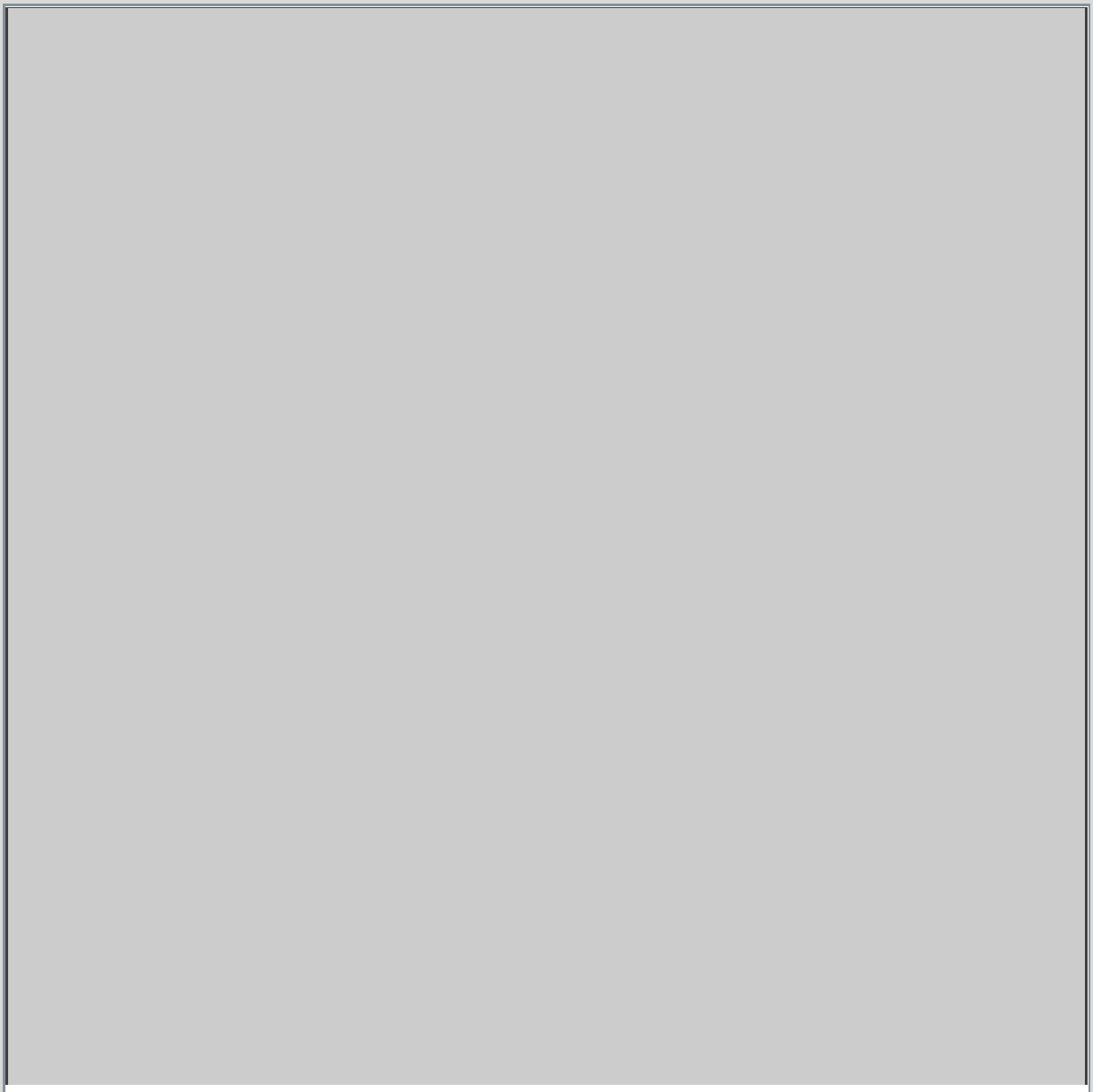
From: NW3C <training@nw3c.org>
To: marissa.sanchezkrug@cookcountyil.gov, Marissa SanchezKrug (Sheriff) <Marissa.SanchezKrug@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:49 PM CDT
Received: June 30, 2020 11:10:52 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

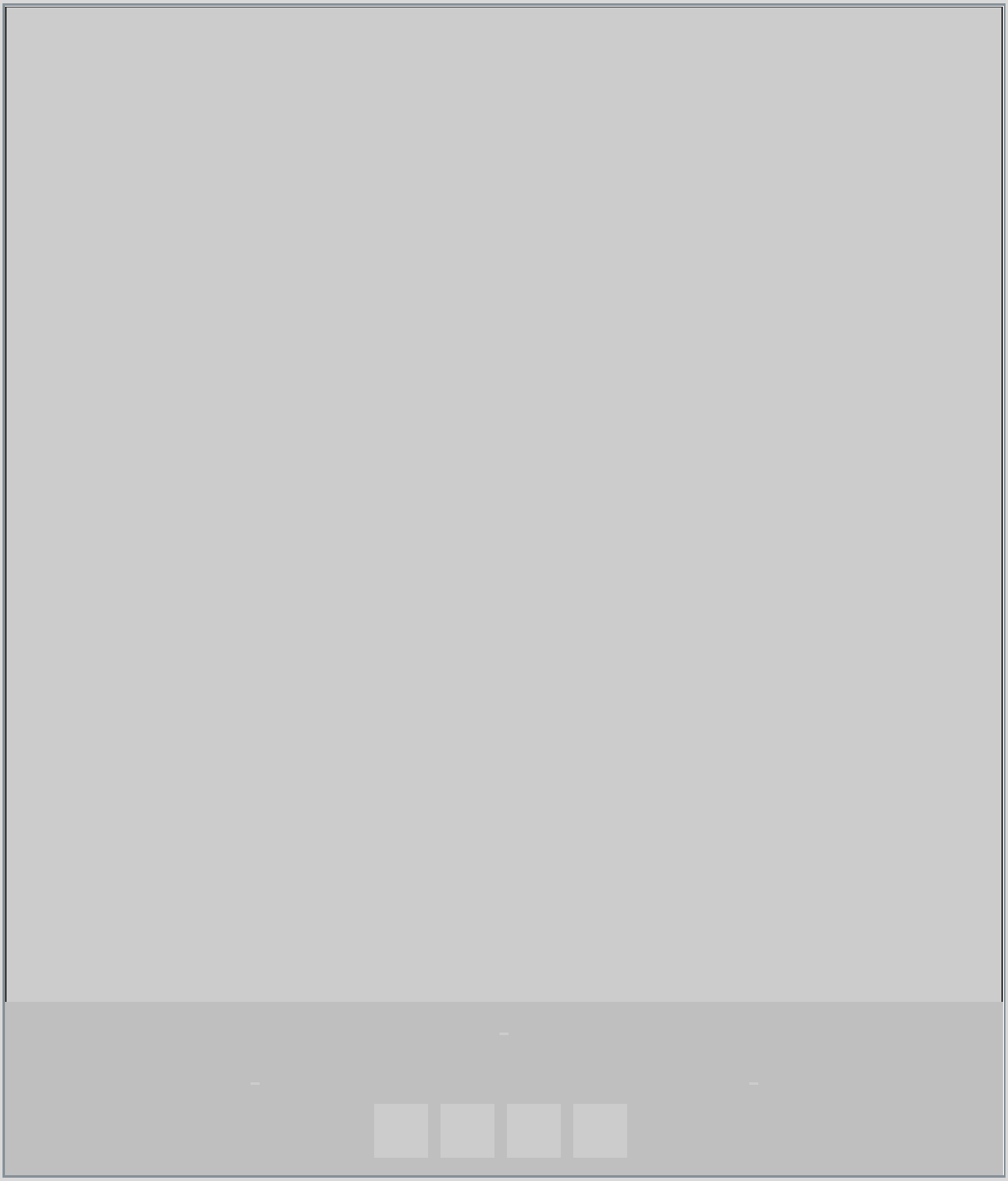
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

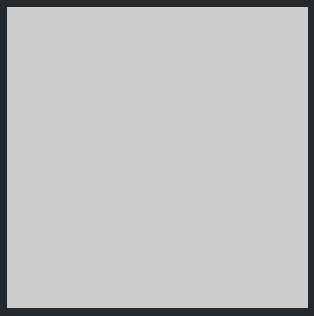
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Marissa SanchezKrug (Sheriff)
Sent:	June 30, 2020 11:10:49 PM CDT
Received:	June 30, 2020 11:10:53 PM CDT

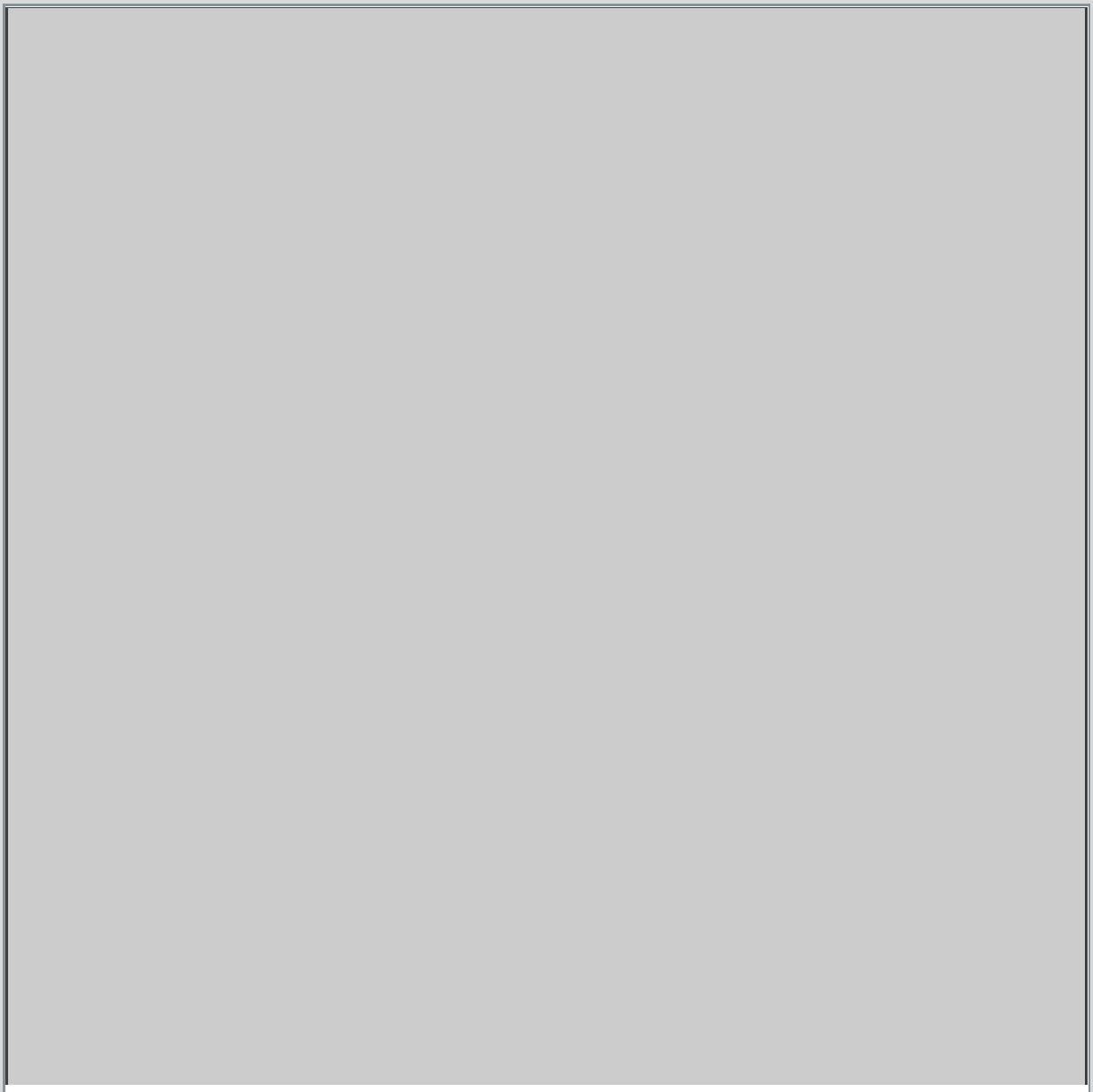
New courses available!

From:	NW3C <training@nw3c.org>
To:	scott.lefko@cookcountyil.gov, Scott Lefko (Sheriff) <Scott.Lefko@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:51 PM CDT
Received:	June 30, 2020 11:10:53 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

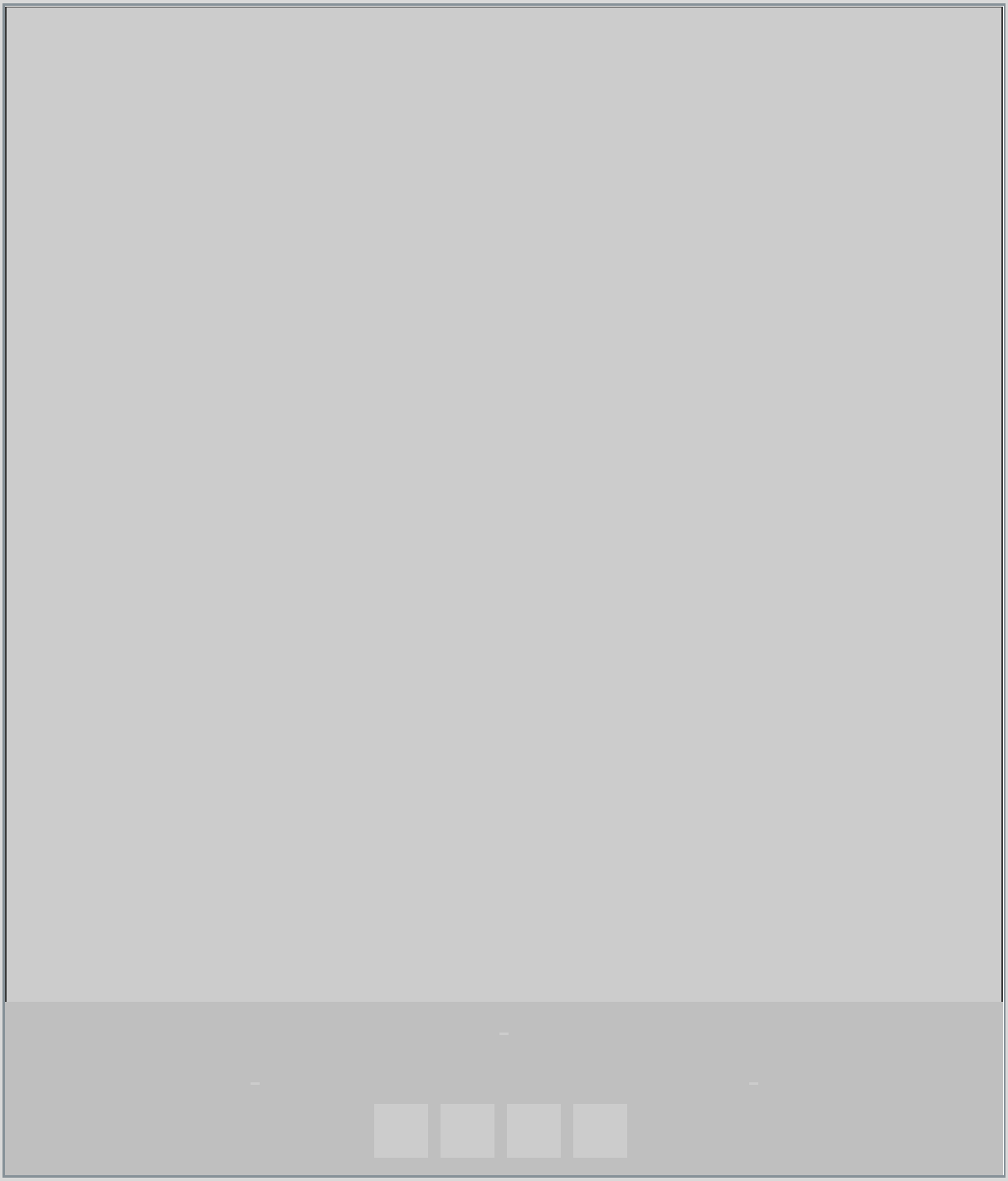
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

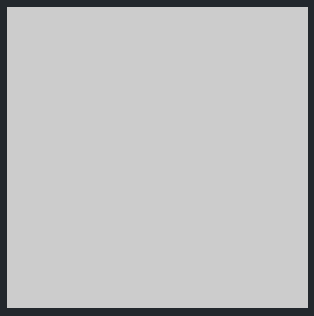
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

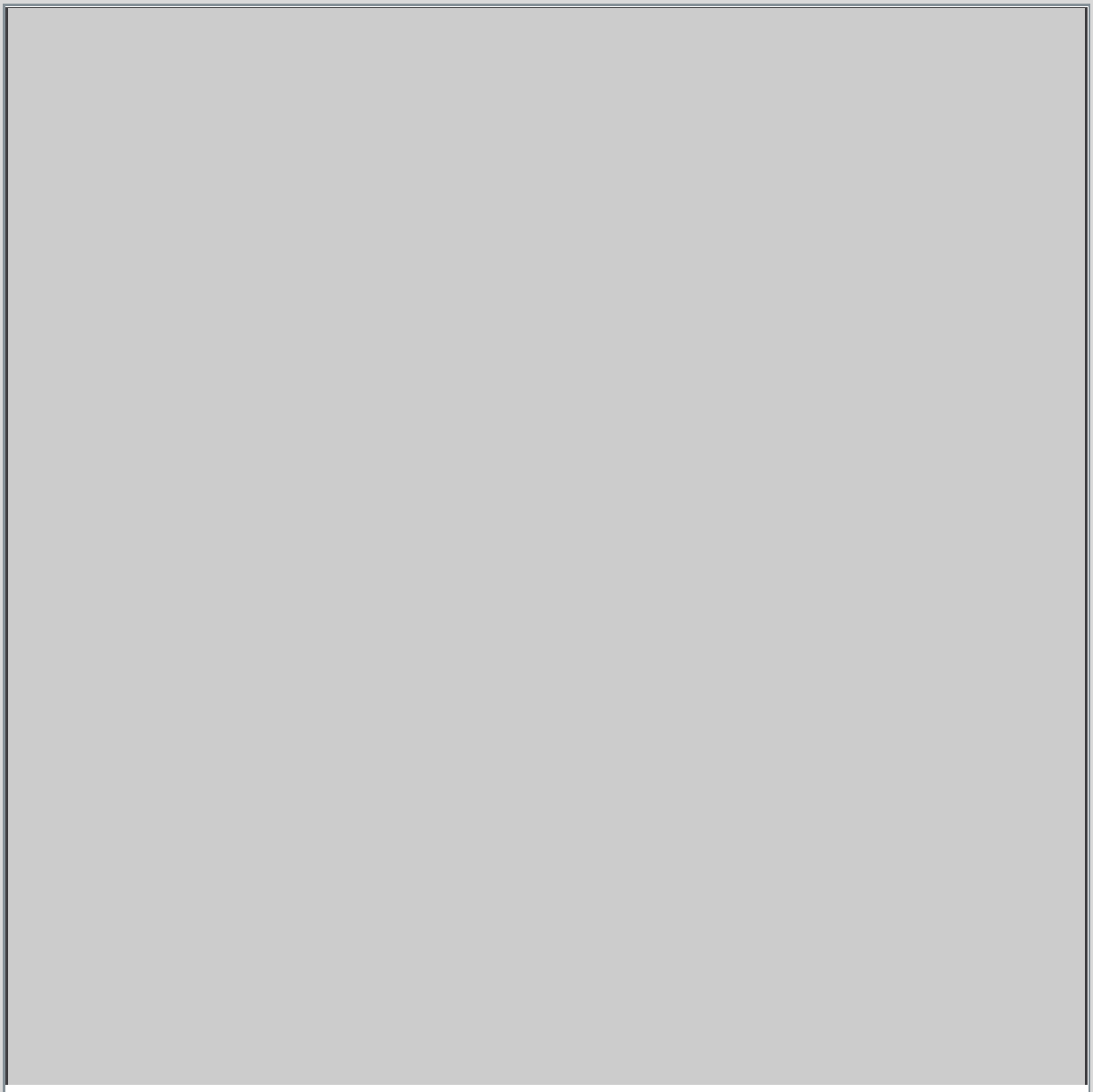
From: NW3C <training@nw3c.org>
To: keith.mccarter@cookcountyil.gov, Keith McCarter (Sheriff) <Keith.McCarter@cookcountyil.gov>
Sender: NW3C <members@nw3c.ccsend.com>

Sent: June 30, 2020 11:10:51 PM CDT
Received: June 30, 2020 11:10:53 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

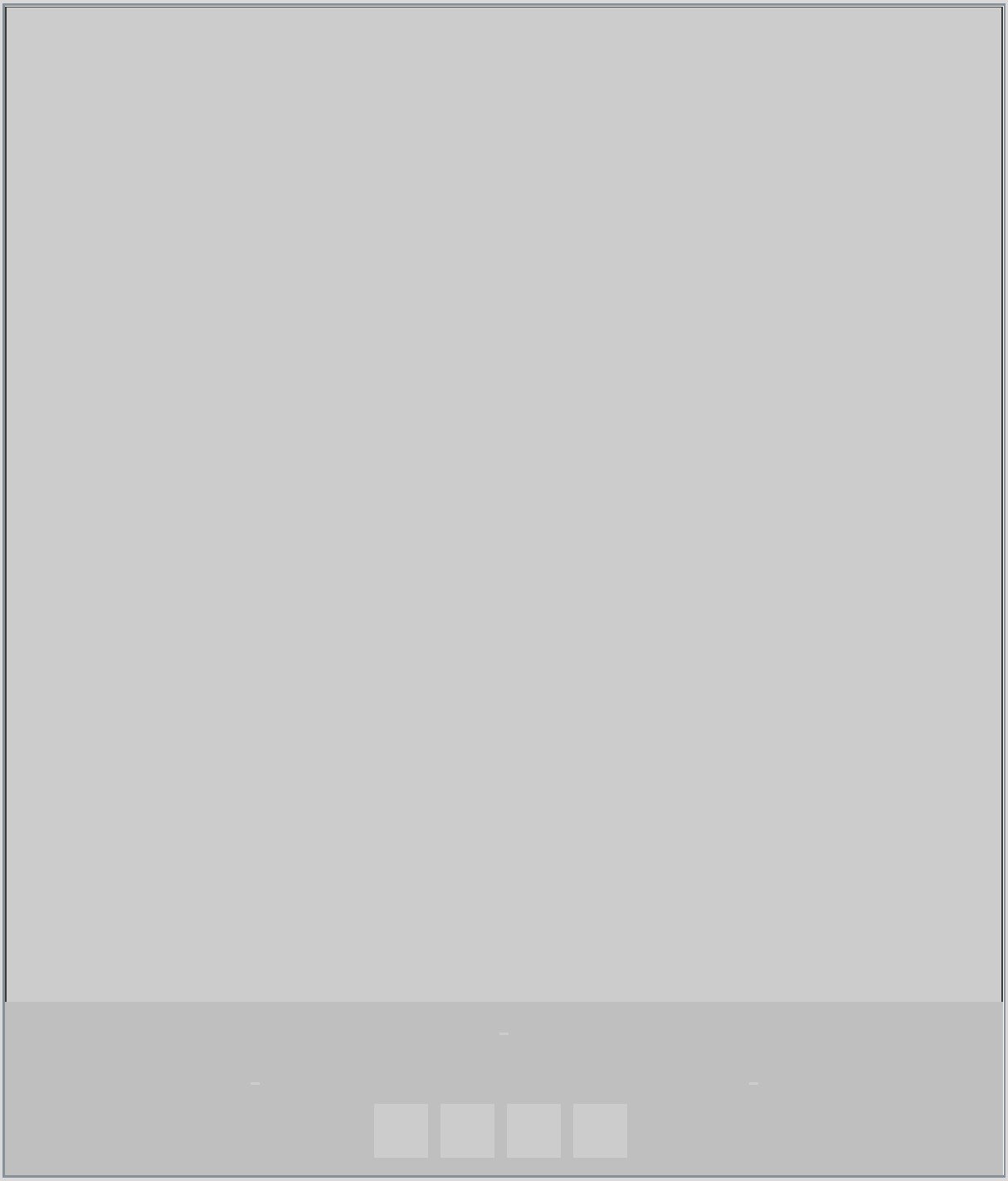
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

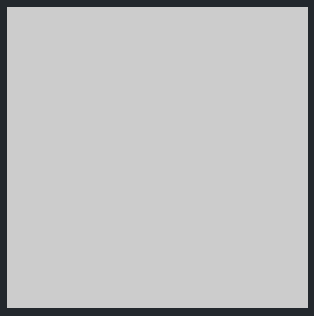
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Keith McCarter (Sheriff)
Sent:	June 30, 2020 11:10:51 PM CDT
Received:	June 30, 2020 11:10:54 PM CDT

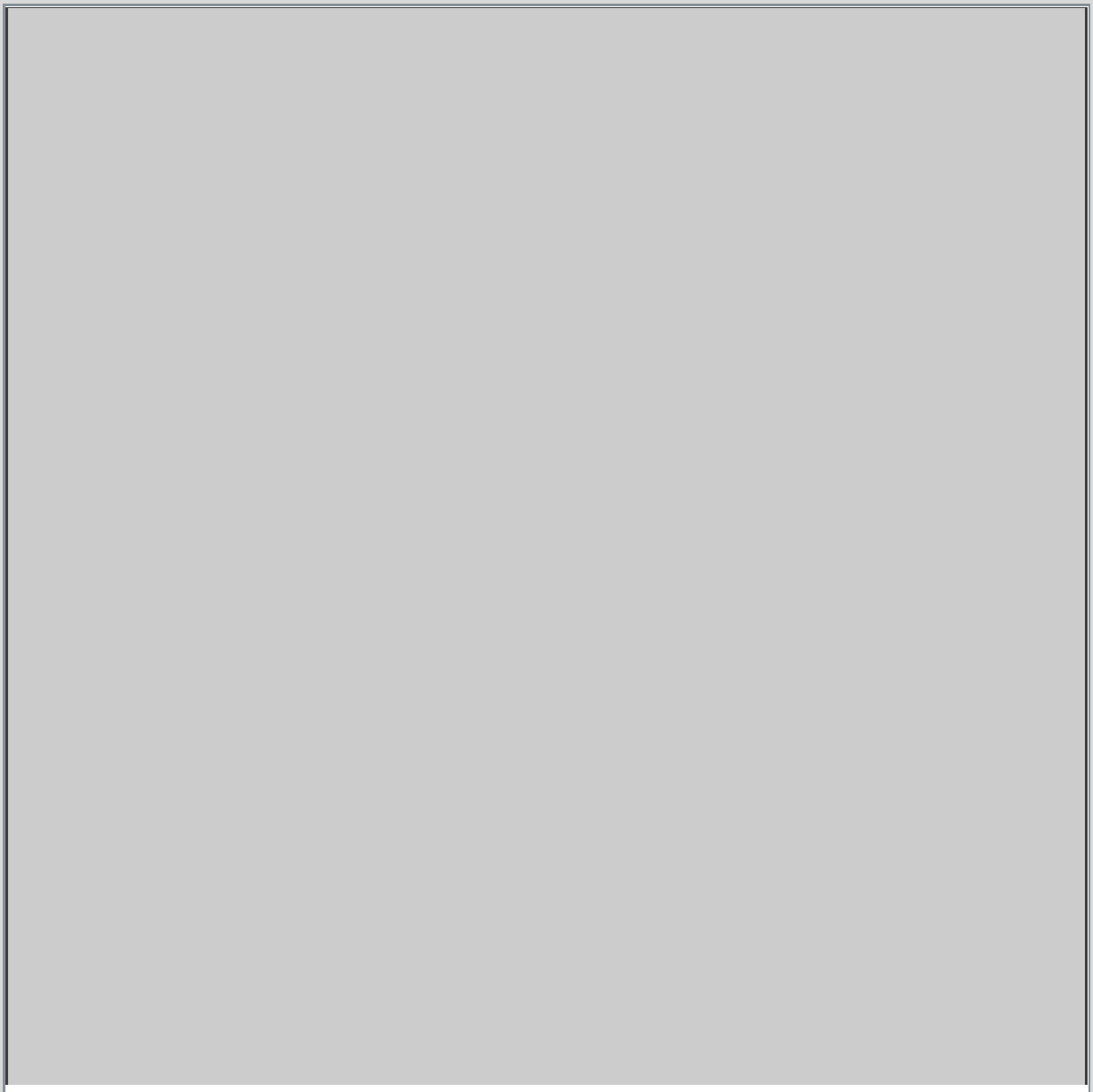
New courses available!

From:	NW3C <training@nw3c.org>
To:	sajid.haidari@cookcountyil.gov, Sajid Haidari (Sheriff) <Sajid.Haidari@cookcountyil.gov>
Sender:	NW3C <members@nw3c.ccsend.com>
Sent:	June 30, 2020 11:10:52 PM CDT
Received:	June 30, 2020 11:10:54 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.





An Agency’s Cybersecurity and the Integrity of Digital Evidence?
Wed, Jul 08, 2020 1:00 PM Eastern

Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration
Thu, Jul 09, 2020 1:00 PM Eastern

OSINT Made Easier: Using Babel Street to more intelligently search PAI for situational awareness and discovery
Tue, Jul 14, 2020 1:00 PM Eastern

What Is There To Know About Credit Card Fraud?
Thu, Jul 16, 2020 3:00 PM Eastern

Did you miss a live webinar?
Check out our on-demand webinars! Available any time for your convenience.

NIST Study for Digital Forensics Experts

Expand Your Opportunities with a Professional Certification

NIST is conducting a study to measure how well the digital forensics community does their job. In this study, you will examine simulated digital evidence and then answer questions that might arise in a real criminal investigation. This study is will help evaluate the scientific foundations of digital forensic methods.

LEARN MORE

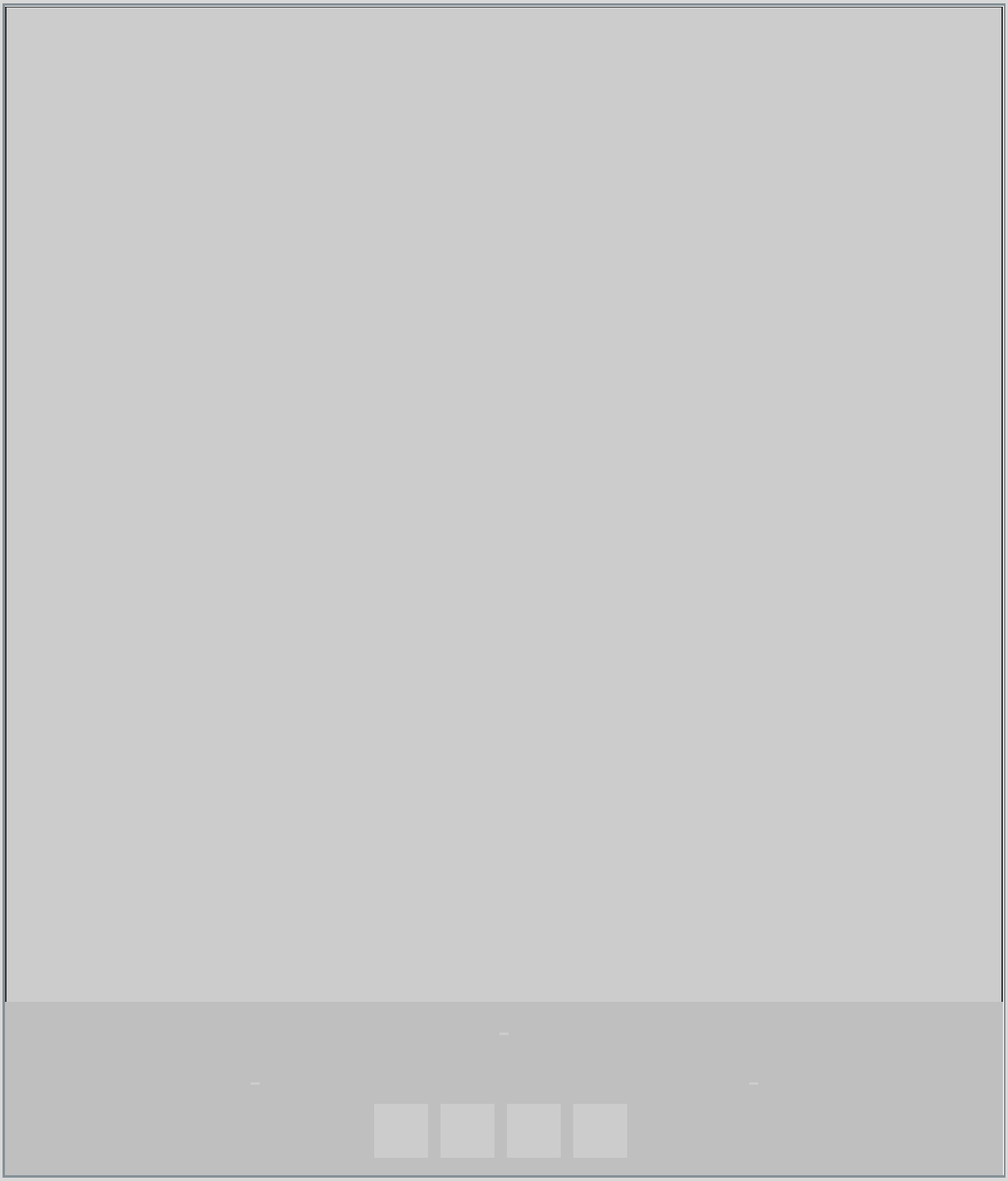
NW3C certifications are designed for professionals in law enforcement and the private sector. Certifications can help you distinguish yourself professionally, obtain the next step in your career, and qualify as a skilled fact or expert witness. Get certified today to expand your opportunities.

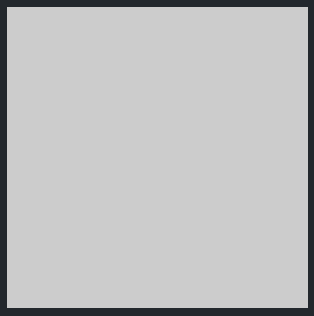
LEARN MORE

BlueLeaks: Law Enforcement Data Leak

Thousands of U.S. police documents were leaked to the public in what's being called "BlueLeaks." Due to this breach, it is recommended that law enforcement agencies and personnel take proper precautions found in this investigative resource. Please login to view the document under OPSEC.

LEARN MORE





Please note: By clicking unsubscribe, you will not receive mass communication from NW3C, Inc. You may still receive important direct communication from NW3C, Inc. related to: service and account changes, products or services for which you have registered, and site cancellation or business termination information.

NW3C | 5000 Nasa Blvd, Suite 2400, Fairmont, WV 26554
Unsubscribe | Privacy Policy

New courses available!

To:	Sajid Haidari (Sheriff)
Sent:	June 30, 2020 11:10:52 PM CDT
Received:	June 30, 2020 11:10:55 PM CDT

UNCLASSIFIED//FOR OFFICIAL USE ONLY//HSIN Intelligence Community Distribution

From: Jasmine Adams (Sheriff) <Jasmine.Adams@cookcountyil.gov>

To: Abraham Yasin (Sheriff) <Abraham.Yasin@cookcountyil.gov>, Tarry Williams (Sheriff) <Tarry.Williams@cookcountyil.gov>, Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov>, Adriana Morales (Sheriff) <Adriana.Morales@cookcountyil.gov>, Alfonzo Hunter (Sheriff) <Alfonzo.Hunter@cookcountyil.gov>, Amanda Gallegos (Sheriff) <Amanda.Gallegos@cookcountyil.gov>, Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Bradley Curry (Sheriff) <Bradley.Curry@cookcountyil.gov>, Brian White (Sheriff) <Brian.White@cookcountyil.gov>, Carmen Gercone (Sheriff) <Carmen.Gercone@cookcountyil.gov>, Carmen Ruffin (Sheriff) <Carmen.Ruffin@cookcountyil.gov>, Christopher Imhof (Sheriff) <Christopher.Imhof@cookcountyil.gov>, David Chiko (Sheriff) <David.Chiko@cookcountyil.gov>, Erik Roedel (Sheriff) <Erik.Roedel@cookcountyil.gov>, Gregory Ernst (Sheriff) <Gregory.Ernst@cookcountyil.gov>, Heather Bock (Sheriff) <Heather.Bock@cookcountyil.gov>, Jennifer Black (Sheriff) <Jennifer.Black@cookcountyil.gov>, Jerry Baldwin (Sheriff) <Jerry.Baldwin@cookcountyil.gov>, John Vega (Sheriff) <John.Vega@cookcountyil.gov>, John Webb (Sheriff) <John.Webb@cookcountyil.gov>, Jonathan Myslinski (Sheriff) <Jonathan.Myslinski@cookcountyil.gov>, Joseph Bellettiere (Sheriff) <Joseph.Bellettiere@cookcountyil.gov>, Kathleen Urbanczyk (Sheriff) <Kathleen.Urbanczyk@cookcountyil.gov>, Kelley Eldridge (Sheriff) <Kelley.Eldridge@cookcountyil.gov>, Kevin Connelly (Sheriff) <Kevin.Connelly@cookcountyil.gov>, Kevin Ruel (Sheriff) <Kevin.Ruel@cookcountyil.gov>, Larry Schurig (Sheriff) <Larry.Schurig@cookcountyil.gov>, Lonnie Hollis (Sheriff) <Lonnie.Hollis@cookcountyil.gov>, Marlon Parks (Sheriff) <Marlon.Parks@cookcountyil.gov>, Matthew Creen (Sheriff) <Matthew.Creen@cookcountyil.gov>, Michael Brady (Sheriff) <Michael.Brady@cookcountyil.gov>, Michael Lucente (Sheriff) <Michael.Lucente@cookcountyil.gov>, Michael Miller (Sheriff) <Michael.Miller1@cookcountyil.gov>, Patrick Dwyer (Sheriff) <Patrick.Dwyer@cookcountyil.gov>, Patrick Moerlien (Sheriff) <Patrick.Moerlien@cookcountyil.gov>, Richard Brogan (Sheriff) <Richard.Brogan@cookcountyil.gov>, Richard O'Brien (Sheriff) <richard.obrien2@cookcountyil.gov>, Robert Lunk (Sheriff) <Robert.Lunk@cookcountyil.gov>, Ronald Jenkins (Sheriff) <Ronald.Jenkins@cookcountyil.gov>, Stephen Bouffard (Sheriff) <Stephen.Bouffard@cookcountyil.gov>, Theodore Stajura (Sheriff) <Theodore.Stajura@cookcountyil.gov>, Jason Hernandez (Sheriff) <Jason.Hernandez@cookcountyil.gov>, James Moore (Sheriff) <James.Moore2@cookcountyil.gov>

Sent: July 1, 2020 9:45:48 AM CDT

Received: July 1, 2020 9:45:49 AM CDT

Attachments: SIN06292020 (U) July 2020 Dates of Significance.pdf, OSIR-04001-0809-20.pdf, OSIR-04001-0808-20.pdf

ALLCON:

Please see attached latest intelligence bulletins from the HSIN Intelligence Community.

Jasmine Adams

Criminal Research Analyst II

Cook County Sheriff's Department

Strategic Operations Center

3026 S California Ave.

Bldg.. 5, 2nd Floor Rm 205

Chicago, Illinois 60608

Email: *jasmine.adams@cookcountyil.gov*

Distribution

To:	Abraham Yasin (Sheriff), Tarry Williams (Sheriff), Leo Schmitz (Sheriff), Adriana Morales (Sheriff), Alfonzo Hunter (Sheriff), Amanda Gallegos (Sheriff), Amar Patel (Sheriff), Bradley Curry (Sheriff), Brian White (Sheriff), Carmen Gercone (Sheriff), Carmen Ruffin (Sheriff), Christopher Imhof (Sheriff), David Chiko (Sheriff), Erik Roedel (Sheriff), Gregory Ernst (Sheriff), Heather Bock (Sheriff), Jennifer Black (Sheriff), Jerry Baldwin (Sheriff), John Vega (Sheriff), John Webb (Sheriff), Jonathan Myslinski (Sheriff), Joseph Bellettiere (Sheriff), Kathleen Urbanczyk (Sheriff), Kelley Eldridge (Sheriff), Kevin Connelly (Sheriff), Kevin Ruel (Sheriff), Larry Schurig (Sheriff), Lonnie Hollis (Sheriff), Marlon Parks (Sheriff), Matthew Creen (Sheriff), Michael Brady (Sheriff), Michael Lucente (Sheriff), Michael Miller (Sheriff), Patrick Dwyer (Sheriff), Patrick Moerlien (Sheriff), Richard Brogan (Sheriff), Richard O'Brien (Sheriff), Robert Lunk (Sheriff), Ronald Jenkins (Sheriff), Stephen Bouffard (Sheriff), Theodore Stajura (Sheriff), Jason Hernandez (Sheriff), James Moore (Sheriff)
Sent:	July 1, 2020 9:45:48 AM CDT
Received:	July 1, 2020 9:45:50 AM CDT

Distribution

To:	Abraham Yasin (Sheriff), Tarry Williams (Sheriff), Leo Schmitz (Sheriff), Adriana Morales (Sheriff), Alfonzo Hunter (Sheriff), Amanda Gallegos (Sheriff), Amar Patel (Sheriff), Bradley Curry (Sheriff), Brian White (Sheriff), Carmen Gercone (Sheriff), Carmen Ruffin (Sheriff), Christopher Imhof (Sheriff), David Chiko (Sheriff), Erik Roedel (Sheriff), Gregory Ernst (Sheriff), Heather Bock (Sheriff), Jennifer Black (Sheriff), Jerry Baldwin (Sheriff), John Vega (Sheriff), John Webb (Sheriff), Jonathan Myslinski (Sheriff), Joseph Bellettiere (Sheriff), Kathleen Urbanczyk (Sheriff), Kelley Eldridge (Sheriff), Kevin Connelly (Sheriff), Kevin Ruel (Sheriff), Larry Schurig (Sheriff), Lonnie Hollis (Sheriff), Marlon Parks (Sheriff), Matthew Creen (Sheriff), Michael Brady (Sheriff), Michael Lucente (Sheriff), Michael Miller (Sheriff), Patrick Dwyer (Sheriff), Patrick Moerlien (Sheriff), Richard Brogan (Sheriff), Richard O'Brien (Sheriff), Robert Lunk (Sheriff), Ronald Jenkins (Sheriff), Stephen Bouffard (Sheriff), Theodore Stajura (Sheriff), Jason Hernandez (Sheriff), James Moore (Sheriff), Arunas Buntinas (Sheriff)
Cc:	Bradley Curry (Sheriff), Marlon Parks (Sheriff), Brian White (Sheriff), Arunas Buntinas (Sheriff), Tarry Williams (Sheriff)
Sent:	July 1, 2020 9:45:48 AM CDT
Received:	July 1, 2020 9:45:50 AM CDT

UNCLASSIFIED//FOR OFFICIAL USE ONLY//HSIN Intelligence Community

Distribution

To:	Abraham Yasin (Sheriff), Tarry Williams (Sheriff), Leo Schmitz (Sheriff), Adriana Morales (Sheriff), Alfonzo Hunter (Sheriff), Amanda Gallegos (Sheriff), Amar Patel (Sheriff), Bradley Curry (Sheriff), Brian White (Sheriff), Carmen Gercone (Sheriff), Carmen Ruffin (Sheriff), Christopher Imhof (Sheriff), David Chiko (Sheriff), Erik Roedel (Sheriff), Gregory Ernst (Sheriff), Heather Bock (Sheriff), Jennifer Black (Sheriff), Jerry Baldwin (Sheriff), John Vega (Sheriff), John Webb (Sheriff), Jonathan Myslinski (Sheriff), Joseph Bellettiere (Sheriff), Kathleen Urbanczyk (Sheriff), Kelley Eldridge (Sheriff), Kevin Connelly (Sheriff), Kevin Ruel (Sheriff), Larry Schurig (Sheriff), Lonnie Hollis (Sheriff), Marlon Parks (Sheriff), Matthew Creen (Sheriff), Michael Brady (Sheriff), Michael Lucente (Sheriff), Michael Miller (Sheriff), Patrick Dwyer (Sheriff), Patrick Moerlien (Sheriff), Richard Brogan (Sheriff), Richard O'Brien (Sheriff), Robert Lunk (Sheriff), Ronald Jenkins (Sheriff), Stephen Bouffard (Sheriff), Theodore Stajura (Sheriff), Jason Hernandez (Sheriff), James Moore (Sheriff), Sheriff Intel
Sent:	July 1, 2020 9:45:48 AM CDT
Received:	July 1, 2020 9:45:50 AM CDT

Distribution

To:	Abraham Yasin (Sheriff), Tarry Williams (Sheriff), Leo Schmitz (Sheriff), Adriana Morales (Sheriff), Alfonzo Hunter (Sheriff), Amanda Gallegos (Sheriff), Amar Patel (Sheriff), Bradley Curry (Sheriff), Brian White (Sheriff), Carmen Gercone (Sheriff), Carmen Ruffin (Sheriff), Christopher Imhof (Sheriff), David Chiko (Sheriff), Erik Roedel (Sheriff), Gregory Ernst (Sheriff), Heather Bock (Sheriff), Jennifer Black (Sheriff), Jerry Baldwin (Sheriff), John Vega (Sheriff), John Webb (Sheriff), Jonathan Myslinski (Sheriff), Joseph Bellettiere (Sheriff), Kathleen Urbanczyk (Sheriff), Kelley Eldridge (Sheriff), Kevin Connelly (Sheriff), Kevin Ruel (Sheriff), Larry Schurig (Sheriff), Lonnie Hollis (Sheriff), Marlon Parks (Sheriff), Matthew Creen (Sheriff), Michael Brady (Sheriff), Michael Lucente (Sheriff), Michael Miller (Sheriff), Patrick Dwyer (Sheriff), Patrick Moerlien (Sheriff), Richard Brogan (Sheriff), Richard O'Brien (Sheriff), Robert Lunk (Sheriff), Ronald Jenkins (Sheriff), Stephen Bouffard (Sheriff), Theodore Stajura (Sheriff), Jason Hernandez (Sheriff), James Moore (Sheriff), Arunas Buntinas (Sheriff)
Sent:	July 1, 2020 9:45:48 AM CDT
Received:	July 1, 2020 9:45:50 AM CDT

Distribution

To:	Abraham Yasin (Sheriff), Tarry Williams (Sheriff), Leo Schmitz (Sheriff), Adriana Morales (Sheriff), Alfonzo Hunter (Sheriff), Amanda Gallegos (Sheriff), Amar Patel (Sheriff), Bradley Curry (Sheriff), Brian White (Sheriff), Carmen Gercone (Sheriff), Carmen Ruffin (Sheriff), Christopher Imhof (Sheriff), David Chiko (Sheriff), Erik Roedel (Sheriff), Gregory Ernst (Sheriff), Heather Bock (Sheriff), Jennifer Black (Sheriff), Jerry Baldwin (Sheriff), John Vega (Sheriff), John Webb (Sheriff), Jonathan Myslinski (Sheriff), Joseph Bellettiere (Sheriff), Kathleen Urbanczyk (Sheriff), Kelley Eldridge (Sheriff), Kevin Connelly (Sheriff), Kevin Ruel (Sheriff), Larry Schurig (Sheriff), Lonnie Hollis (Sheriff), Marlon Parks (Sheriff), Matthew Creen (Sheriff), Michael Brady (Sheriff), Michael Lucente (Sheriff), Michael Miller (Sheriff), Patrick Dwyer (Sheriff), Patrick Moerlien (Sheriff), Richard Brogan (Sheriff), Richard O'Brien (Sheriff), Robert Lunk (Sheriff), Ronald Jenkins (Sheriff), Stephen Bouffard (Sheriff), Theodore Stajura (Sheriff), Jason Hernandez (Sheriff), James Moore (Sheriff), Michael Aliperti, Ben Spear
Sent:	July 1, 2020 9:45:48 AM CDT
Received:	July 1, 2020 9:45:50 AM CDT

UNCLASSIFIED//FOR OFFICIAL USE ONLY//HSIN Intelligence Community

Distribution

To:	Abraham Yasin (Sheriff), Tarry Williams (Sheriff), Leo Schmitz (Sheriff), Adriana Morales (Sheriff), Alfonzo Hunter (Sheriff), Amanda Gallegos (Sheriff), Amar Patel (Sheriff), Bradley Curry (Sheriff), Brian White (Sheriff), Carmen Gercone (Sheriff), Carmen Ruffin (Sheriff), Christopher Imhof (Sheriff), David Chiko (Sheriff), Erik Roedel (Sheriff), Gregory Ernst (Sheriff), Heather Bock (Sheriff), Jennifer Black (Sheriff), Jerry Baldwin (Sheriff), John Vega (Sheriff), John Webb (Sheriff), Jonathan Myslinski (Sheriff), Joseph Bellettiere (Sheriff), Kathleen Urbanczyk (Sheriff), Kelley Eldridge (Sheriff), Kevin Connelly (Sheriff), Kevin Ruel (Sheriff), Larry Schurig (Sheriff), Lonnie Hollis (Sheriff), Marlon Parks (Sheriff), Matthew Creen (Sheriff), Michael Brady (Sheriff), Michael Lucente (Sheriff), Michael Miller (Sheriff), Patrick Dwyer (Sheriff), Patrick Moerlien (Sheriff), Richard Brogan (Sheriff), Richard O'Brien (Sheriff), Robert Lunk (Sheriff), Ronald Jenkins (Sheriff), Stephen Bouffard (Sheriff), Theodore Stajura (Sheriff), Jason Hernandez (Sheriff), James Moore (Sheriff), Sheriff Intel, Arunas Buntinas (Sheriff)
Cc:	Bradley Curry (Sheriff), Marlon Parks (Sheriff), Brian White (Sheriff), Arunas Buntinas (Sheriff), Tarry Williams (Sheriff)
Sent:	July 1, 2020 9:45:48 AM CDT
Received:	July 1, 2020 9:45:50 AM CDT

UNCLASSIFIED//FOR OFFICIAL USE ONLY//HSIN Intelligence Community Distribution

From:	Jasmine Adams (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=846708BEE1C64CC1ABD023D2F5F7264E-JASMINE ADA>
To:	Abraham Yasin (Sheriff) <Abraham.Yasin@cookcountyil.gov>, Tarry Williams (Sheriff) <Tarry.Williams@cookcountyil.gov>, Leo Schmitz (Sheriff) <Leo.Schmitz@cookcountyil.gov>, Adriana Morales (Sheriff) <Adriana.Morales@cookcountyil.gov>, Alfonzo Hunter (Sheriff) <Alfonzo.Hunter@cookcountyil.gov>, Amanda Gallegos (Sheriff) <Amanda.Gallegos@cookcountyil.gov>, Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Bradley Curry (Sheriff) <Bradley.Curry@cookcountyil.gov>, Brian White (Sheriff) <Brian.White@cookcountyil.gov>, Carmen Gercone (Sheriff) <Carmen.Gercone@cookcountyil.gov>, Carmen Ruffin (Sheriff) <Carmen.Ruffin@cookcountyil.gov>, Christopher Imhof (Sheriff) <Christopher.Imhof@cookcountyil.gov>, David Chiko (Sheriff) <David.Chiko@cookcountyil.gov>, Erik Roedel (Sheriff) <Erik.Roedel@cookcountyil.gov>, Gregory Ernst (Sheriff) <Gregory.Ernst@cookcountyil.gov>, Heather Bock (Sheriff) <Heather.Bock@cookcountyil.gov>, Jennifer Black (Sheriff) <Jennifer.Black@cookcountyil.gov>, Jerry Baldwin (Sheriff) <Jerry.Baldwin@cookcountyil.gov>, John Vega (Sheriff) <John.Vega@cookcountyil.gov>, John Webb (Sheriff) <John.Webb@cookcountyil.gov>, Jonathan Myslinski (Sheriff) <Jonathan.Myslinski@cookcountyil.gov>, Joseph Bellettiere (Sheriff) <Joseph.Bellettiere@cookcountyil.gov>, Kathleen Urbanczyk (Sheriff) <Kathleen.Urbanczyk@cookcountyil.gov>, Kelley Eldridge (Sheriff) <Kelley.Eldridge@cookcountyil.gov>, Kevin Connelly (Sheriff) <Kevin.Connelly@cookcountyil.gov>, Kevin Ruel (Sheriff) <Kevin.Ruel@cookcountyil.gov>, Larry Schurig (Sheriff) <Larry.Schurig@cookcountyil.gov>, Lonnie Hollis (Sheriff) <Lonnie.Hollis@cookcountyil.gov>, Marlon Parks (Sheriff) <Marlon.Parks@cookcountyil.gov>, Matthew Creen (Sheriff) <Matthew.Creen@cookcountyil.gov>, Michael Brady (Sheriff) <Michael.Brady@cookcountyil.gov>, Michael Lucente (Sheriff) <Michael.Lucente@cookcountyil.gov>, Michael Miller (Sheriff) <Michael.Miller1@cookcountyil.gov>, Patrick Dwyer (Sheriff) <Patrick.Dwyer@cookcountyil.gov>, Patrick Moerlien (Sheriff) <Patrick.Moerlien@cookcountyil.gov>, Richard Brogan (Sheriff) <Richard.Brogan@cookcountyil.gov>, Richard O'Brien (Sheriff) <richard.obrien2@cookcountyil.gov>, Robert Lunk (Sheriff) <Robert.Lunk@cookcountyil.gov>, Ronald Jenkins (Sheriff) <Ronald.Jenkins@cookcountyil.gov>, Stephen Bouffard (Sheriff) <Stephen.Bouffard@cookcountyil.gov>, Theodore Stajura (Sheriff) <Theodore.Stajura@cookcountyil.gov>, Jason Hernandez (Sheriff) <Jason.Hernandez@cookcountyil.gov>, James Moore (Sheriff) <James.Moore2@cookcountyil.gov>
Sent:	July 1, 2020 9:45:48 AM CDT
Received:	June 30, 2020 4:36:00 PM CDT
Attachments:	SIN06292020 (U) July 2020 Dates of Significance.pdf, OSIR-04001-0809-20.pdf, OSIR-04001-0808-20.pdf

ALLCON:

Please see attached latest intelligence bulletins from the HSIN Intelligence Community.

Jasmine Adams

Criminal Research Analyst II

Cook County Sheriff's Department

Strategic Operations Center

3026 S California Ave.

Bldg.. 5, 2nd Floor Rm 205

Chicago, Illinois 60608

Email: jasmine.adams@cookcountyil.gov

FW: (U/LES) TAM-C Situation Report United States: 1 July 2020 #2

From:	Thomas Tilton (Emergency Management) <Thomas.Tilton@cookcountyil.gov>
To:	Robert Lunk (Sheriff) <Robert.Lunk@cookcountyil.gov>, Michael Brady (Sheriff) <Michael.Brady@cookcountyil.gov>
Sent:	July 1, 2020 1:14:20 PM CDT
Received:	July 1, 2020 1:14:29 PM CDT
Attachments:	TAM-C Situation Report United States_ 1 July 2020 #2.xlsx, PACIC CIKR_WPAHFC JIB - ANIMAL AGRICULTURE FACILITY LOCATIONS DISCLOSED ON INTERACTIVE WEBSITE.pdf, 2020_07_01.pdf, (U FOUO) DHS CSAC Chemical Current News Report - 20200701.pdf, (U FOUO) TSA IA UPFRONT - 20200630.pdf, (U FOUO) TSA Surface Complaince Analysis Network (SCAN) 06242020 to 07012020 - 20200701.pdf, (U) US Dept. of Transportation – Daily Open Source Reporting - 20200701.pdf, DSR (0391-20) 1 Jul 20 - Final.pdf, MTI Project SP0520 (06.07).pdf, OSINT 20200701.pdf, SP 0520 RB (06.28).pdf

FYI

From: Ness, Michael <michael.ness@hq.dhs.gov>
Sent: Wednesday, July 01, 2020 1:11 PM
To: Adrian Cunningham (Adrian.Cunningham@fema.dhs.gov); 'Adrianne.Michele@socom.mil'; AITES, KELLIE A CIV USAF ACC 55 SFS/S5AT <kellie.aites@us.af.mil>; 'Allen_Rothbaum@ios.doi.gov'; Anderson, Matthew E LT USN STRATCOM J34 (USA) (matthew.e.anderson5.mil@mail.mil) <matthew.e.anderson5.mil@mail.mil>; Distler, Andrew (CTR) <andrew.distler@associates.hq.dhs.gov>; MARCUS, ANDREW <andrew.marcus@hq.dhs.gov>; Anna Castillo <anna.castillo.1@us.af.mil>; Brad Tippit (Brad.Tippit@Missouricitytx.gov) <Brad.Tippit@Missouricitytx.gov>; 'Bruce.Steven.Miller@us.army.mil'; Pelton, Bryan (CTR) <bryan.pelton@associates.hq.dhs.gov>; 'captain@berwickpolice.org'; Chandra White <Chandra.white@us.af.mil>; Oppliger, Christopher <christopher.oppliger@hq.dhs.gov>; Cisneros, Tony <Tony.Cisneros@fletc.dhs.gov>; 'CLTibbs@co.pg.md.us'; ALFORD, DALE <dale.alford@hq.dhs.gov>; 'Darryl_Ward@ios.doi.gov'; ATWOOD, DAVID (CTR) <david.atwood@associates.hq.dhs.gov>; Davidson, Jeffrey <jeffrey.davidson@hq.dhs.gov>; Delcore, Robert <Robert.Delcore@uscis.dhs.gov>; Delgado, Jose L <Jose.Delgado@tsa.dhs.gov>; 'dennis.gonzalez@CityofRochester.gov'; dgirou@arlingtonva.us; 'dgpeterson@lanl.gov'; Schwarzrock, Don <don.schwarzrock@hq.dhs.gov>; Downey, Michael <Michael.Downey@hq.dhs.gov>; Dzurilla, Christopher <Christopher.Dzurilla@HQ.DHS.GOV>; Gagnon, Bruce P <Bruce_Gagnon@nps.gov>; Graves, Jeremy W MSgt USAF AFDW (USA) (jeremy.w.graves.mil@mail.mil) <jeremy.w.graves.mil@mail.mil>; greg.brock@nlrb.gov; HARDING, DANIEL <daniel.harding@hq.dhs.gov>; Harvey, Timothy <Timothy.Harvey@fletc.dhs.gov>; Henry Rivero: <Henry.Rivero@bep.gov>; 'hhgreen@nmic.navy.mil'; Holder, Richard <Richard.Holder@HQ.DHS.GOV>; Hughes, Gregory (CDC/OPHSS/NCHS) (nvx2@cdc.gov) <nvx2@cdc.gov>; Hunter, Joseph David (Joe) 2d LT USAF (US) (joseph.d.hunter16.mil@mail.mil) <joseph.d.hunter16.mil@mail.mil>; CURRIE, JASON (CTR) <jason.currie@associates.hq.dhs.gov>; Jeffrey McClung <jeffrey.mcclung@jfcc-imd.stratcom.mil>; Henderson, Jesse K CTR <Jesse.K.Henderson@uscg.mil>; Tadrick, Joe <Joe.Tadrick@hq.dhs.gov>; John Bamford <Jbamford@arlingtonva.us>; 'john.a.kavaliunas.civ@mail.mil'; 'John.Glodo@crystal.dia.mil'; 'john.leo-1@nasa.gov'; Jonesmcgee, Darius A SSgt USAF (USA) (darius.a.jonesmcgee.mil@mail.mil) <darius.a.jonesmcgee.mil@mail.mil>; JS Pentagon DoM Mailbox JSSO Military Security Force <js.pentagon.dom.mbx.jsso-military-security-force@mail.mil>; kenneth.j.anderson3.civ@mail.mil; Kristy KorchakCampbell (kristy.korchakcampbell@us.af.mil) <kristy.korchakcampbell@us.af.mil>; kristy.korchak-campbell@auab.afcent.af.mil; 'kunichs@guestservices.com'; Battiste, Lawrence <lawrence.battiste@hq.dhs.gov>; Lee Taylor (Lee.Taylor@hq.dhs.gov); Linneman, Eric <Eric.linneman@dla.mil>; Mannix, Alan <Alan.Mannix@bep.gov>; 'mark.holloway@ic.fbi.gov'; Marler, Christopher F SSgt USAF (USA) (christopher.f.marler.mil@mail.mil) <christopher.f.marler.mil@mail.mil>; Mascolo, John <John.Mascolo@tsa.dhs.gov>; 'Matthew.f.croson@usdoj.gov'; McBride, Chip <chip.mcbride@hq.dhs.gov>; Michael Malcolm <michael.s.malcolm2.civ@mail.mil>; Michael Robinson: <michael.robinson@bep.gov>; 'michael.g.copeland2.civ@mail.mil'; Michael.Kenny@bep.gov; 'michael.w.young8.ctr@mail.mil'; Mike Evans <Mike.Evans@calvertcountymd.gov>; monika.l.junker.civ@mail.mil; Moreta, Richard <richard.moreta@hq.dhs.gov>; Nicholas Paoletti (nicholas.paoletti.1@us.af.mil) <nicholas.paoletti.1@us.af.mil>; 'n-nc.peterson.ncj3.mbx.j34-letic-omb@mail.mil'; 'Odis.Stroud@cookcountyil.gov'; Oppermann, George Henry CIV USARMY USAG (US) <george.h.oppermann.civ@mail.mil>; Ortega, John A CIV <John.A.Ortega@uscg.mil>; Booker, Patrick M (N/A)

<patrick.m.booker@uscis.dhs.gov>; Patterson, Richard V (Rick) CTR STRATCOM J34 (US) <richard.v.patterson.ctr@mail.mil>; Pepin, Andrew <Andrew.Pepin@HQ.DHS.GOV>; Groven, Philip <Philip.Groven@hq.dhs.gov>; Ping, William Darion <william.d.ping.civ@mail.mil>; Pinkham, Lawrence H JR CIV STRATCOM J34 (US) <lawrence.h.pinkham.civ@mail.mil>; 'PittmanT@state.gov'; POULSEN, ROBERT A 2d Lt USAF ACC 55 ISS/IN <robert.poulsen@us.af.mil>; 'Raymond.Hankins@nlrb.gov'; Loveless, Richard <richard.loveless@hq.dhs.gov>; Richard Reed <Richard.Reed@firstnet.gov>; Richard Swarens <Richard.Swarens@whmo.mil>; 'Richard.Cestero@bep.gov'; Roddy, Gene E. CIV WHMO/HQ <Gene.E.Roddy@whmo.mil>; Russell, John W MSG USARMY JS DOM (US) <john.w.russell36.mil@mail.mil>; 'russell.r.hicks.civ@mail.mil'; BOYER, RYAN <ryan.boyer@hq.dhs.gov>; 'Ryan.Gibson@faa.gov'; 'Salvatore.ingraldi.civ@mail.mil'; Shell, Alvin <alvin.shell@bep.gov>; Sims, Karen <karen.sims@hq.doe.gov>; 'smithbr@state.gov'; Stephen J Barbieri (stephen.j.barbieri@uscis.dhs.gov); Stephen Kunich <Stephen.Kunich@pae.com>; 'Stephen.Hutchens@bep.gov'; Steven Schoen <steven.m.schoen@lmco.com>; Stewart, Kerry <Kerry.Stewart@cisa.dhs.gov>; Stewart, Kevin L CTR <Kevin.L.Stewart@uscg.mil>; 'sylvia.c.harris.civ@mail.mil'; Thomas Klug: <Thomas.Klug@bep.gov>; 'thomas.a.stroud@nasa.gov'; 'thomas.loyd@uscp.gov'; 'Thomas.Tilton@cookcountyil.gov'; Torian, William A Jr CIV USAF (USA) (william.a.torian.civ@mail.mil) <william.a.torian.civ@mail.mil>; Versichelli, Thomas <thomas.versichelli.civ@mail.mil>; Victor Calloway <vcalloway@gpo.gov>; Waage, Timothy S CIV STRATCOM J34 (US) <timothy.s.waage.civ@mail.mil>; Waterman, Ronald T CIV DSS DSS ISFO (US) <ronald.t.waterman.civ@mail.mil>; BERG, WENDY <wendy.berg@hq.dhs.gov>; WERNER, MATTHEW R TSgt USAF AFOSI 55 SFS/Det 204 <matthew.werner.4@us.af.mil>; Wilemon, Nicole <nwilemon@blm.gov>; DeArcangelis, William <william.dearcangelis@HQ.DHS.GOV>; Balcerzak, William J <William.J.Balcerzak@uscis.dhs.gov>; Wilson, Randall Craig CIV USARMY 21 SIG BDE (USA) (randall.c.wilson12.civ@mail.mil) <randall.c.wilson12.civ@mail.mil>; Wolf, Thomas John (Tom) CIV USARMY 21 SIG BDE (US) (thomas.j.wolf.civ@mail.mil) <thomas.j.wolf.civ@mail.mil>; Wyman, Isabel <isabel.wyman@hq.dhs.gov>
Subject: FW: (U/LES) TAM-C Situation Report United States: 1 July 2020 #2

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Michael "Elliot" Ness
Program Manager
Industrial Security Branch – CCIPP Program Office
Office of Chief Security Officer | National Security Services Division |
DHS-HQ Desk: 202-447-5046 | Mobile Work Cell: 202-853-0569
Email(s): michael.ness@hq.dhs.gov, or OCSO-SARM@hq.dhs.gov

Homeland Security

"With honor and integrity, we will safeguard the American people, our homeland, and our values."

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator. This communication, along with any attachments, is covered by Federal and State law governing electronic communications and may contain restricted and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message.

From: McIntyre, Timothy A <Timothy.A.McIntyre@ice.dhs.gov>
Sent: Wednesday, July 1, 2020 11:42 AM
To: Ness, Michael <michael.ness@hq.dhs.gov>
Subject: (U/LES) TAM-C Situation Report United States: 1 July 2020 #2

Please see below identified upcoming events throughout the United States in connection to the death of George Floyd in Minneapolis on 25 May 2020.

Region	City	Date	Time (Local Time)	Lat	Lng	Details
California	Alameda	7/3/2020	10:00LT and 17:00LT	37.767066	-122.242998	On 3 July 2020, at 10:00LT and 17:00LT, activists in Alameda, CA, will stage a die in protest in front of the Alameda police station at 1555 Oak St (37.767066, -122.242998).
Georgia	Atlanta	7/2/2020	17:30 LT	33.740149	-84.345412	On 2 July 2020, at 17:30 LT, activists in Atlanta, GA, intend to protest at the intersection of Flat Shoals and Glenwood Avenues (33.740149, -84.345412).
Indiana	Decatur	7/3/2020	18:30LT	40.829509	-84.929288	On 3 July 2020, at 18:30LT, activists in Decatur, IN, will stage a protest in 618 W Madison St (40.829509, -84.929288).
Indiana	South Bend	7/2/2020	11:30 LT	41.683323	-86.250128	On 2 July 2020, at 11:30 LT, activists in South Bend, IN, plan to protest outside of the

						Memorial Hospital, located at 602 S Michigan Street (41.683323, -86.250128).
Maine	Bath	7/2/2020	17:00 LT	43.912807	-69.813777	On 2 July 2020, at 17:00 LT, activists in Bath, ME, intend to protest outside of City Hall (43.912807, -69.813777).
Massachusetts	Jamaica Plain	7/2/2020	17:30 LT	42.313781	-71.11474	On 2 July 2020, at 17:30 LT, activists in Jamaica Plain, MA plan to protest outside of the First Baptist Church in Jamaica Plain, located at 633 Centre Street (42.313781, -71.114740).
New York	Brooklyn	7/3/2020	19:00LT	40.673888	-73.969678	On 3 July 2020, at 19:00LT, activists in Brooklyn, NY, will stage a protest at the Grand Army Plaza (40.673888, -73.969678).
New York	New Rochelle	7/3/2020	16:00LT	40.929425	-73.793772	On 3 july 2020, at 16:00LT, activists in New Rochelle, NY, will hold a march from the New Rochelle High School

						(40.929425, -73.793772) to Quaker Ridge Rd (40.947389, -73.795969).
North Carolina	Wilmington	7/2/2020	17:00LT	34.237058	-77.945888	On 2 July 2020, at 17:00LT, activists in Wilmington, NC, plan to gather at 102 North 3rd Street (34.237058, -77.945888).
North Carolina	Wilmington	7/3/2020	17:00LT	34.237058	-77.945888	On 3 July 2020, at 17:00LT, activists in Wilmington, NC, plan to gather at 102 North 3rd Street (34.237058, -77.945888).
Oklahoma	Oklahoma City	7/2/2020	09:00 LT	35.469493	-97.515184	On 2 July 2020, at 09:00 LT, activists in Oklahoma City, OK, intend to protest in Kerr Park (35.469493, -97.515184).
Oregon	Oak Grove	7/2/2020	17:00 LT	45.415813	-122.631741	On 2 July 2020, at 17:00 LT, activists in Oak Grove, OR, intend to protest at the intersection of Oak Grove Boulevard and McLoughlin Boulevard (45.415813, -122.631741).
Oregon	Portland	7/2/2020	12:00LT	45.569932	-	On 2 July

					122.687374	2020, at 12:00LT, activists in Portland, OR, plan to gather at in the corner of N Rosa Parks Ways and N Denver Avenue (45.569932, -122.687374).
Oregon	Portland	7/3/2020	12:00LT	45.569932	-122.687374	On 3 July 2020, at 12:00LT, activists in Portland, OR, plan to gather at in the corner of N Rosa Parks Ways and N Denver Avenue (45.569932, -122.687374).
Pennsylvania	Allentown	7/2/2020	15:30 LT	40.597724	-75.488029	On 2 July 2020, at 15:30 LT, activists in Allentown, PA, intend to gather at the intersection of 15th Street and Hamilton Street (40.597724, -75.488029).
Rhode Island	West Warwick	7/2/2020	16:30 LT	41.707184	-71.515405	On 2 July 2020, at 16:30 LT, activists in West Warwick, RI, will hold a protest at 100 Factory Street (41.707184, -71.515405).
Texas	Dallas	7/2/2020	18:00LT	32.776428	-96.797088	On 2 July 2020, at 18:00LT, activists in

						Dallas, TX, will stage a protest in front of the City Hall (32.776428, -96.797088).
Texas	Dallas	7/3/2020	18:00LT	32.776428	-96.797088	On 3 July 2020, at 18:00LT, activists in Dallas, TX, will stage a protest in front of the City Hall (32.776428, -96.797088).
Texas	Denton	7/2/2020	14:00LT and 18:00LT	33.215034	-97.132987	On 2 July 2020, at 14:00LT and 18:00LT, activists in Denton, TX, plan to hold two protests at Courthouse-on-the-Square Museum (33.215034, -97.132987).
Texas	Denton	7/3/2020	14:00LT and 18:00LT	33.215034	-97.132987	On 3 July 2020, at 14:00LT and 18:00LT, activists in Denton, TX, plan to hold two protests at Courthouse-on-the-Square Museum (33.215034, -97.132987).
Washington	Tacoma	7/2/2020	17:00 LT	47.224418	-122.472874	On 2 July 2020, at 17:00 LT, activists in Tacoma, WA, intend to protest in front of the

						Tacoma Police Department's headquarters, located at 3701 S Pine Street (47.224418, -122.472874).
Wyoming	Cheyenne	7/3/2020	17:00LT	41.140277	-104.820354	On 3 July 2020, at 17:00LT, activists in Cheyenne, WY, will stage a protest in front of the Wyoming State Capitol Building (41.140277, -104.820354).

--

TAM-C Operations
operations@tamcintel.com
24/7: +1.202.922.0068
https://www.tamc365.com/

This email transmission and any accompanying attachments may contain TAM-C Solutions privileged and confidential information intended only for the use of the intended addressee. Any dissemination, distribution, copying or action taken in reliance on the contents of this email by anyone other than the intended recipient is strictly prohibited. If you have received this email in error please immediately delete it and notify sender at the above TAM-C Solutions email address. Sender and TAM-C Solutions accept no liability for any damage caused directly or indirectly by receipt of this email.

FW: (U/LES) TAM-C Situation Report United States: 1 July 2020 #2

To:	Robert Lunk (Sheriff), Michael Brady (Sheriff), Abraham Yasin (Sheriff), Tarry Williams (Sheriff), Leo Schmitz (Sheriff), Adriana Morales (Sheriff), Alfonzo Hunter (Sheriff), Amanda Gallegos (Sheriff), Amar Patel (Sheriff), Bradley Curry (Sheriff), Brian White (Sheriff), Carmen Gercone (Sheriff), Carmen Ruffin (Sheriff), Christopher Imhof (Sheriff), David Chiko (Sheriff), Erik Roedel (Sheriff), Gregory Ernst (Sheriff), Heather Bock (Sheriff), Jennifer Black (Sheriff), Jerry Baldwin (Sheriff), John Vega (Sheriff), John Webb (Sheriff), Jonathan Myslinski (Sheriff), Joseph Bellettiere (Sheriff), Kathleen Urbanczyk (Sheriff), Kelley Eldridge (Sheriff), Kevin Connelly (Sheriff), Kevin Ruel (Sheriff), Larry Schurig (Sheriff), Lonnie Hollis (Sheriff), Marlon Parks (Sheriff), Matthew Creen (Sheriff), Michael Lucente (Sheriff), Michael Miller (Sheriff), Patrick Dwyer (Sheriff), Patrick Moerlien (Sheriff), Richard Brogan (Sheriff), Richard O'Brien (Sheriff), Ronald Jenkins (Sheriff), Stephen Bouffard (Sheriff), Theodore Stajura (Sheriff), Jason Hernandez (Sheriff), James Moore (Sheriff)
Sent:	July 1, 2020 1:14:20 PM CDT
Received:	July 1, 2020 1:14:31 PM CDT

FW: (U/LES) TAM-C Situation Report United States: 1 July 2020 #2

To:	Robert Lunk (Sheriff), Michael Brady (Sheriff)
Sent:	July 1, 2020 1:14:20 PM CDT
Received:	July 1, 2020 1:14:29 PM CDT

INFO - bomb 1,2,3,4

From:	Mike Grimes <mgrimes@butlersheriff.org>
To:	Mike Grimes <mgrimes@butlersheriff.org>
Sent:	July 2, 2020 12:01:42 PM CDT
Received:	July 2, 2020 12:05:47 PM CDT
Attachments:	202006-SAB-015.pdf, 2021 Flyer Final.pdf, CBRNE & Vulnerable Targets Bi-Monthly Digest April - May 2020.pdf, NYPD_Weekly Terrorism Brief_26 June 2020_SHIELD.pdf, (FOUO) COVID-19 - Worldwide - Situation Report - 07-01-20 (Update 109).pdf, SHIELD - Event Threat Assessment - 2020 Macys Fourth of July Fireworks.pdf

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

FYI and hope you all have a safe 4th of July !!

Here is a link to the CPSC list of overloaded fireworks: https://www.cpsc.gov/recalls

mg

G Michael Grimes
Bomb Squad Commander
Butler County Sheriff's Office
705 Hanover Street
Hamilton, OH 45011

Disp) 513.785.1300
Off) 513.785.1006
Fax) 513.785.1220
Cell) 513.200.6664

[GovQA] 1 Day Reminder - R009142-062920

From: Cook County Sheriff's Office <cookcountysheriff@govqa.us>
To: Elizabeth.Scannell@cookcountyil.gov, Elizabeth Scannell (Sheriff) <Elizabeth.Scannell@cookcountyil.gov>
Sent: July 3, 2020 8:00:51 AM CDT
Received: July 3, 2020 8:00:55 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Reminder the following request is due in ONE (1) business days: FOIA Request / R009142-062920
Please log in to the FOIA Request Center to review this request and update as needed.

Request Information
Assigned Staff: Elizabeth Scannell
Status: Received
Create Date: 6/29/2020 3:37:05 AM
Record(s) Requested: To Whom It May Concern: Pursuant to the Illinois Freedom of Information Act., I hereby request the following records: 1. Documents mentioning, describing or generated in response to the BlueLeaks release, the preceding hack or subsequent fallout, including but not limited to: * Damage assessments * Emails * Interagency communications (local, state, or federal) * Communications with the press about BlueLeaks * Communications with Twitter or other social media or sharing platforms 2. Documents mentioning or describing Distributed Denial of Secrets (DDoSecrets) You may limit this request to records generated between November 1, 2018 and the present. I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers in outlets such as Gizmodo, MuckRock, Motherboard, Property of the People, Unicorn Riot, and The Outline, among others. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the library Internet Archive and the journalist non-profit MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself. As such, it is not necessary for me to demonstrate the relevance of this particular subject in advance. As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived. The requested documents will be made available to the general public, and this request is not being made for commercial purposes. In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not. Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 5 business days, as the statute requires. Sincerely, Emma Best Upload documents directly:
https://https://www.muckrock.comhttps://accounts.muckrock.com/accounts/login/?next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fcook-county-sheriff-719%252Fblueleaks-cook-county-sheriff-96941%252F%253F&url_auth_token=AAAaaJnszUVssmdgx6fh2R-tE3U%3A1jppAE%3ADWZbgy7n864OATjAMxtAsPZltYs
Login to the system and view this request by clicking View the Request

This is an auto-generated email and has originated from an unmonitored email account. Please DO NOT REPLY

[GovQA] 1 Day Reminder - R009142-062920

To:	Elizabeth Scannell (Sheriff)
Sent:	July 3, 2020 8:00:51 AM CDT
Received:	July 3, 2020 8:00:55 AM CDT

CSWR-20025 CrowdStrike Intelligence Weekly Report: Week of 06/27/2020

From: intel-notifications@crowdstrike.com
To: keith.morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: July 3, 2020 3:26:37 PM CDT
Received: July 3, 2020 3:26:40 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.



CSWR-20025 CrowdStrike Intelligence Weekly Report: Week of 06/27/2020

On 22 July 2020, CrowdStrike Intelligence will host the Q2 Executive Briefing, an interactive session that will examine some of the notable activity and trends observed during April, May, and June. Briefing topics will include:

- Global Geopolitical Review
- Sector Threat Highlight: Telecommunications
- Update on Ransomware and Data Leaks
- INDRIK SPIDER: Post Indictment Changes
- WICKED PANDA: Attribution Challenges Posed with Cobalt Strike

Registration details for the Q2 Executive Briefing will be forthcoming soon.

Analysis Reveals CARBON SPIDER Use of REvil; JSS Loader Distribution Campaign Observed

Multiple instances of *REvil* (developed by PINCHY SPIDER) activity in conjunction with *Cobalt Strike* have been attributed with medium confidence by CrowdStrike Intelligence to CARBON SPIDER (CSA-200830). The activity suggests the adversary is monetizing access to networks without Point-of-Sale (PoS) systems by encrypting them with ransomware. The assessment is based on overlaps in tooling, infrastructure, and motivation. In particular, multiple connections were made through Cobalt Strike samples using the unique license identifier 452436291.

Separately, on 29 June 2020, CrowdStrike Intelligence identified a *Leo VBS* (CSA-191224) distribution campaign delivering *JSS Loader* (CSA-191197). While neither Leo VBS nor JSS Loader are unique to a particular adversary, it is likely this campaign was conducted by CARBON SPIDER. This assessment carries moderate confidence based on the combination of Tactics, Techniques, and Procedures (TTPs) and observed command-and-control (C2) infrastructure (CSA-200844).

Criminal Actor Installs Pharmaceutical-Themed Spam Pages on Compromised Web Server

On 25 June 2020, CrowdStrike Falcon OverWatch observed hands-on activity conducted by a criminal actor at a North America-based academic institution. The initial infection vector of the incident is unknown, but the hands-on-activity reveals interesting information about the actors TTPs (CSA-200834). Throughout 25 and 26 June, the criminal actor performed reconnaissance activity on the host by checking if their session was being debugged, locating the web root, and retrieving user account names. The actor proceeded to use `wget` to retrieve a ZIP archive from a remote location and decompressed the archive into the web root. The ZIP archive was over 500MB in size and contained more than 30,000 pharmaceutical-themed web pages advertising various medications available for online purchase without a prescription.

Reportedly New Ransom X Ransomware is Identified as Defray777

On 26 June 2020, security researchers published a report stating that a new ransomware named *Ransom X* had been used in an operation against a U.S.-based government transportation department. CrowdStrike Intelligence has obtained and analyzed samples of the reportedly new ransomware and has identified the family as the existing *Defray777* (CSA-200835).

Though security researchers use the name Defray777 to refer to this ransomware, the internal binary name set at compile time—`ransom.exx`—led to the name Ransom X. The new sample displays an updated ransom note format. Previously observed Defray777 ransom notes included an alternate contact method using BitMessage; however, this is no longer present in the new ransom note. The updated note includes updated instructions for the victim; however, the instruction to "contact someone from IT department" remains the same as in previous ransom notes.

New Ragnar Locker Victim Post Provides Insight to TTPs; Indications of Collaborations Between BGH Operators

A recent post by VIKING SPIDER on their dedicated leak site (DLS) detailing a new victim has provided insight to the operator's TTPs (CSA-200822). The post alludes to the actors exploiting vulnerabilities to secure initial access and moving laterally through the network after successfully elevating permissions to "Domain admin" level. Although the exact vulnerabilities exploited are unconfirmed, the information provides important insights to VIKING SPIDER's modus operandi.

There is increasing evidence of a collaboration or business relationship between VIKING SPIDER and the big game hunting (BGH) operators TWISTED SPIDER. Earlier in June, the two adversaries hosted victim information from each other's operations on their DLSs (CSA-200745). Both have reiterated their intent to refrain from targeting healthcare entities during the current pandemic, and both draw attention to their victims' security issues. This collaborative activity is unique in the current BGH threat landscape, with Ransomware-as-a-Service (RaaS) and affiliate programs the more commonly observed business arrangement.

Spam Campaign Mimicking Italian Revenue Agency Distributes Gozi ISFB

An Italian-language spam campaign involving emails mimicking the Italian Revenue Agency was observed on 29 June 2020 distributing the *Gozi ISFB* banking trojan (CSA-200842). The emails included Excel 4.0 macro documents, and referenced two articles of Italian legislation regarding tax refunds—the timing of the campaign was highly likely intended to coincide with Italy's annual tax deadline of 30 June. Phishing campaigns involving Excel 4.0 macro documents have become increasingly popular during 2020 (CSA-200461). In contrast to typical macro documents, which contain Visual Basic for Applications (VBA) macros, these documents use Excel 4.0 macros that predate VBA macros. It is likely adversaries are using Excel 4.0 macro documents to evade email and host-based security tools that are likely optimized to detect and prevent embedded VBA macros.

DanaBot Sub-Botnet 4 Distributing Avaddon Ransomware

SCULLY SPIDER's *DanaBot* sub-botnet 4 was observed by CrowdStrike Intelligence distributing *Avaddon* ransomware between 22 and 30 June 2020 (CSA-200846). This is the first instance of the sub-botnet delivering this ransomware variant—previous payloads delivered by sub-botnet 4 include WIZARD SPIDER's *Trickbot*, SMOKY SPIDER's *SmokeBot*, and various information stealers and remote administration tools (RATs).

Avaddon has previously been distributed in spam campaigns, including one campaign in June 2020 involving the *Phorpiex* malware targeting Japanese email addresses (CSA-200752). This Avaddon campaign was seemingly opportunistic, with no explicit sector or geographic focus identified.

INDRIK SPIDER's WastedLocker Continues to Grow Victim Base; BGH Operators Continue to Add Victim Details to DLS

INDRIK SPIDER has continued to target organizations primarily in the UK and North America using their new ransomware variant *WastedLocker* (CSA-200824). CrowdStrike Intelligence sensitive source reporting has confirmed 22 victims to date, with the manufacturing sector the most heavily targeted. Despite the naming of two key members of INDRIK SPIDER in unsealed indictments and others in financial sanctions, the group has continued to show resilience in their campaigns. *BitPaymer* operations have not been observed since mid-March 2020, and distribution of *Dridex* was last observed in late March 2020 (CSA-200403). The development and use of WastedLocker is likely intended to distance INDRIK SPIDER from their previous Dridex and BitPaymer operations—though similarities between BitPaymer and WastedLocker suggest such separation has not been fully achieved.

Alongside the identification of new WastedLocker victims, several other BGH operators added details of their victims to their associated DLS this week (see Figure 1).

Figure 1. BGH Ransomware Victims by Sector and Country (26 June to 2 July 2020)

Commodity Malware Updates and Underground Forum Activity; Stolen Datasets Advertised for Sale

Several updates, new releases, and advertisements were identified by CrowdStrike Intelligence within the past week on various criminal and underground forums for commodity malware variants (see summary in Table 1).

DATE	MALWARE	DETAILS
24 June 2020	Taurus Project Stealer	Update to newly released v1.4 • New panel includes loader statistics • Filter added for file grabber function • Wasabi and Daedalus collection added • Domain Detect redesigned
24 June 2020	Raccoon Stealer	Updates made to two versions: • Minor fixes and improvements to v1.5.12 • Added Chromium-based Microsoft Edge browser support for v1.5.13 • Bug fixed affecting auto-encryption in v1.5.13 • Downtime planned between 1 and 4 July 2020 for back-end update
25 June 2020	Buer Loader	Updates for v1.3.7 • Runtime cleaning • Added a loader directory for Windows Defender exceptions • Updated anti-virus
26 June 2020	Avaddon Ransomware	Updates to the build, including • Minor improvements and bug fixes • Panel access updated Ongoing recruitment for “networkers” Vendor urged customers to update to the latest version

26 June 2020	Triumph Loader	Update to v1.2.1 • Small update to the boot-loader • General improvements to the loader
29 June 2020	Amadey Loader	Update to v1.90 • File upload algorithm redesigned, and number of attempts to contact command-and-control (C2) server increased to 5 • Loader will reattempt at later date if target server is busy
29 June 2020	Oski Stealer	Update to v1.9.1, whereby helper DLLs downloaded from C2 are now obfuscated

Table 1. Commodity Malware Updates and Adverts

Also identified by CrowdStrike Intelligence sensitive sources are advertisements for various stolen datasets. These advertisements provide a snapshot of the type of information available to purchase or acquire from eCrime adversaries that can be used to perform phishing attacks or other fraudulent activity.

- A user on an underground forum known for database dumps and leaks recently shared a link to a dataset sourced from an Indian e-commerce platform. The data included personally identifiable information (PII) and contact details, including telephone numbers and postal addresses.
- On 26 June 2020, an Iranian eCrime actor advertised for sale the business credit card details for a U.S.-based commercial real estate company. The details were priced at $120 USD.
- A user with a proven track record of selling stolen government and academia-related databases advertised in June 2020 the sale of a database allegedly sourced from the Saudi Ministry of Interior. The data includes passport details, user records, and some travel-related information. The dataset is priced at $1,000 USD.

The Operators of Joker's Stash and Brian's Club Release Multiple Offerings of Compromised Payment Card Information with PII

The operators of Joker's Stash card shop released one offering from their three recent major breaches this week, BIGBADABOOM-III-US-part57. CrowdStrike Intelligence expects the weekly release of compromised payment card data from the NEW WORLD ORDER, BIGBADABOOM-III, and NIRVANA (releases advertised as LOTUS) breaches to continue, based on the historical activity of Joker's Stash card shop. Additionally, the operators of Joker's Stash released four offerings of compromised payment card data that contained personally PII from the U.S., EU, and other unspecified regions of the world. The abbreviation VBV in the offering highly likely indicates that it contains additional information to successfully bypass or complete Verified by Visa (VBV) fraud protection.

DATE	RELEASE NAME	REGION	NO. OF CARDS
27 June 2020	BIGELEPHANT-FULLINFO-	U.S./EU/World	10,000

	DOB-VBV		
29 June 2020	PINEAPPLE-FULLINFO-DOB-VBV	U.S./EU/World	15,000
30 June 2020	BEAUTIFULLIFE-FULLINFO-DOB-VBV	U.S./EU/World	15,000
1 July 2020	CULTURALSHOCK-FULLINFO-MIX	U.S./EU/World	1,000
1 July 2020	BIGBADABOOM-III-US-part57	U.S.	

Table 2. Recent Joker's Stash Card Shop Releases for 25 June - 2 July 2020

From 25 June to 2 July 2020, CrowdStrike Intelligence sources observed the card shop Brian's Club post five releases of compromised payment card information containing PII and included the cardholder's date of birth (DOB) and Social Security number (SSN).

DATE	RELEASE NAME	REGION	PII
25 June 2020	0625_US_IP_SSN	U.S.	DOB, SSN
26 June 2020	0626_US_IP_SSN	U.S.	DOB, SSN
27 June 2020	0627_US_IP_SSN	U.S.	DOB, SSN
28 June 2020	0628_US_IP_SSN	U.S.	DOB, SSN
29 June 2020	0629_US_IP_SSN	U.S.	DOB, SSN

Table 3. Brian's Club PII Offerings for 25 June- 2 July 2020

TARGETED INTRUSION

WICKED PANDA Deploys RouterGod Malware in Targeted Attacks Against Southeast Asian Entities

As part of ongoing targeted activity against Southeast Asian entities, CrowdStrike Falcon OverWatch detected the deployment of novel malware, named *RouterGod*, at an entity associated with the aviation industry in Hong Kong. This malware has likely been used to target entities in Hong-Kong, Macau, and Taiwan with the actor also deploying additional tools such as *Cobalt Strike*, *DarkShell*, and *Proxip* as part of the same campaign. The Proxip and Cobalt Strike samples are configured to use subdomains of `livehost[.]live`, a domain used by WICKED PANDA as part of ShadowPad activity targeting Hong Kong-based universities in 2019 (CSA-200151). Because of the re-use of this low prevalence domain, continued targeting of Southeast Asian entities as well as the deployment of Proxip and Cobalt Strike in tandem, CrowdStrike Intelligence currently attributes this activity to WICKED PANDA with high confidence.

The name RouterGod is used internally by the malware developers, likely due to the ability of the malware to route encrypted command packets between infected hosts. RouterGod is a .NET executable that can be used to execute arbitrary scripts as well as establish sessions with other infected hosts. Multiple instances of the malware can be used in a chain to deliver implant tasking to specific endpoints within victim networks. Additional technical analysis is available in CSA-200848.

Novel Malware Families Loosely Linked to China Identified

This week, CrowdStrike Intelligence released initial analytic findings on newly identified malware. Both malware families were used in operations consistent with Chinese state-nexus activity:

- In June 2020, CrowdStrike Falcon OverWatch observed an unknown adversary deploy novel malware as part of an attempted compromise at a Southeast Asian IT services provider. The deployed malware uses a legitimate antivirus product executable to gain execution via dynamic link library (DLL) search-order hijacking in order to execute a malicious loader DLL that, in turn, decrypts and loads an associated payload file. Additional activity observed included the execution of a Cobalt Strike stager executable that was used to download an additional payload as well as PowerShell commands used to contact unknown infrastructure. See CSA-200849 for more information.

- Also in June 2020, CrowdStrike Falcon OverWatch identified two closely related incidents at an East Asian multinational pharmaceutical company. Both instances featured a previously unseen implant linked to activity CrowdStrike has assessed as consistent with Chinese state interests. For this activity, legitimate VirtualBox executables were used to host malicious DLLs that in turn load and deobfuscate the malicious payloads. See CSA-200833 for more information.

IMPERIAL KITTEN Continues Operations Against Probable Saudi Arabian Technology Organizations with New FireBAK Variant

CrowdStrike Intelligence has identified continued activity from the Iranian state-nexus IMPERIAL KITTEN adversary throughout the first half of 2020. The activity consisted of the apparent continued development of its *FireBAK* implant, with new variants written in PowerShell and Visual Basic Script (VBS). Additional deployment of the adversary's custom *LaZagne* variant were identified in late June 2020. Additional data suggests that current IMPERIAL KITTEN operations likely focus on technology-related organizations in Saudi Arabia. For more information, see CSA-200843.

New LampCarrier Cluster Activity and Infrastructure Identified

CrowdStrike Intelligence has discovered previously unidentified activity attributed to the LampCarrier cluster including Golang-based malware, a Microsoft Office document containing a malicious macro, and previously unidentified infrastructure. Previously observed LampCarrier activity did not include malware as a significant part of its toolset, as the actor preferred to rely on living-off-the land techniques. The discovery of new malware and malicious documents indicates LampCarrier is evolving its TTPs, particularly in how it establishes persistence on victim networks. Additional information and Indicators of Compromise (IOCs) are available in CSA-200831.

HACKTIVISM

MENA Hacktivists Engage in Doxxing and Defacement Activity

On 28 June 2020, hacktivist group *Oman Hackers* claimed to have doxxed more than 20 individuals they believe responsible for managing social media accounts conducting information operations against Omani interests. The vast majority of the purportedly doxxed individuals were Emirati,

although some citizens of other countries in the Middle East and North Africa (MENA) were also identified. The Oman Hackers group claim to have obtained this information by compromising a fake account managed by one of the doxxed individuals and then identifying additional accounts involved in coordinating inauthentic behavior. In particular, the Oman Hackers group focused its doxxing efforts on three individuals whom the group believes to have ties to various Emirati government and security institutions as well as some legal and media organizations. The Oman Hackers group is currently highly active, continuing to claim that an organized conspiracy is harming the Omani government, its regime, and the country's relations with neighboring countries. For more information, see CSA-200836.

Throughout June 2020, hacktivists operating under the moniker *Moroccan Revolution* have reported more than 1200 notifications to the website defacement archive Zone-H. While the group has been active since at least 2015, June 2020 marked a significant increase in defacement claims. Only two of the defacements listed in Zone-H records noted defacements of government websites in June, both of which were in Vietnam. The defacement activity is very likely opportunistic in nature rather than specifically targeted, due to the large number of defacements with no clear geographic or sector targeting theme. While CrowdStrike Intelligence has not independently attributed the geographic origins of most members claiming association with the group, Moroccan Revolution likely consists broadly of North African hacktivists or individuals sympathetic to issues in the region. Additional information is available in CSA-200828.

Fallout from BlueLeaks Release of Sensitive U.S. Law Enforcement Data

On 19 June 2020, hacktivist-journalist entity Distributed Denial of Secrets (*DDOS*) released 269 GB of materials belonging to hundreds of law enforcement agencies across the U.S., naming the collection BlueLeaks (CSA-200801). The release coincided with protests against U.S. law enforcement agencies after the killing of George FLOYD on 25 May and follows similar protests against law enforcement in Latin America (LATAM). Journalist and operator of DDOS Emma BEST—known to work closely with sophisticated hacktivist MOLOTOV JACKAL and has an established track record of publishing materials in the advancement of anti-capitalist and other ideologies (CSA-200663)—made an open call for breaches of U.S. police forces, requesting that hacktivists leak any exfiltrated data to DDOS (CSA-200697). BlueLeaks leveraged at least three simultaneous means of access and distribution: a searchable web portal, a Tor mirror for the portal, and a downloadable Torrent file for the full collection; recent leaks of sensitive law enforcement data in LATAM were published in a similar manner, with a user-friendly GUI enabling easier digestion of the data (CSIT-19233).

Among the BlueLeaks data were sensitive documents belonging to the Maine Information and Analysis Center (MIAC). Internal MIAC communication was allegedly not compromised but results of requests for information (RFIs) were exposed, including personally identifiable information (PII) of subjects and victims as well as information regarding ongoing investigations in Maine. It was also revealed that MIAC has been closely tracking Black Lives Matter (BLM) events and advocacy groups (CSDR-20075).

Hacktivist Campaign Protests Colombian Military Scandal

On 26 June 2020, hacktivist group *Anonymous Colombia* posted an English-language video announcing a campaign to protest acts of extreme violence seven Colombian soldiers committed against indigenous children. The group claimed credit for a DDoS attack and website defacement against two separate websites belonging to former Colombian president and current Senator Álvaro URIBE. A separate hacktivist group known as *Anonym0us China* backed the campaign, claiming responsibility for a DDoS attack of the Colombian Army's English and Spanish-language websites. This operation was the second Anonymous-linked #OpColombia campaign announced that week;

there has been no observed overlap between the actors claiming the activities, highlighting the decentralized nature of the Anonymous movement. For more information, see CSA-200839.

Iranian Hacktivists Target Israeli, U.S. Based Entities

Iranian hacktivist group *Death Squads* claimed credit for a DDoS attack against the domains of an Israeli domain registrar and a U.S.-based bank. As the veracity and credibility of these attacks cannot be confirmed, the attack and associated denial of service were likely limited in duration and effect. Death Squads' latest claims represent a departure from past efforts and are assessed to likely be geopolitically motivated due to the group's nationalistic outlook and the backgrounds of its core membership. This effort is likely of low sophistication and representative of a singular hacktivist effort rather than part of a wider campaign. See CSA-200837 for more information.

The timing of the claim also coincides with additional (though apparently unrelated) attacks claimed by Iranian hacktivist groups *Vortex Security Team* and *Unidentified Security Team* against Israel. Specifically, the groups claimed what appear to be two distinct alleged intrusions: one targeting an Israeli gas company's server and the other against an unknown entity. The server is assessed to likely have been identified via exposed services or port-scanning activity; the propensity of hacktivists to conflate publicly available information with data breaches suggests there are even chances the extent of the intrusion was either exaggerated or extremely limited in scale. The hacktivist groups claim that a 27 June explosion near an Iranian military base on 24 June was a result of an Israeli cyberattack, and the groups took retaliatory action in response. For further reading, see CSA-200840.

DATA EXPOSURE & BREACHES

Threat Actor Reportedly Selling Data Stolen From 14 Companies

A threat actor is reportedly selling databases stolen from 14 different companies on an underground forum, according to media reports.[1] Stolen data varies per company, though all breaches reportedly include usernames and hashed passwords. The threat actor is selling the databases at varying prices, ranging from $100 to $1,100 USD. The companies were all allegedly breached in 2020, though the exact dates of compromise, if true, remains unknown. Of the fourteen companies, four companies have previously reported breaches. It is currently unclear if the stolen databases from those four companies are connected to the previously reported breaches.

Eight U.S. Cities Reportedly Impacted by Click2Gov Breaches

The local governments of eight U.S.-based cities discovered a JavaScript (JS) skimmer had been injected into the payment portals of their Click2Gov sites.[2] The eight cities were located across three U.S. states. Industry researchers disclosed two different exfiltration servers that hosted the JS skimmer; one server was used for three sites and one used for the remaining five sites. The JS skimmer was designed to collect payment card information, including card number, expiration date, and CVV, as well as names and physical addresses. Media reports speculate that these compromises are the result of a threat group leveraging *Magecart* tactics. However, CrowdStrike Intelligence does not currently attribute this activity to a known adversary at this time.

Recent Reporting

CSIT-20100 Analysis of TRACER KITTEN DNSDAT Malware Targeting the Middle Eastern Telecommunications Sector

This Tipper provides technical analysis of the *DNSDAT* malware in use by the Iranian actor TRACER KITTEN.

CSMR-20005 CrowdStrike Intelligence Monthly Report - May 2020

This report provides significant analytic findings from May 2020, including trends observed in targeted intrusion, eCrime, and hacktivist operations.

[1] https[:]//www.bleepingcomputer[.]com/news/security/seller-floods-hacker-forum-with-data-stolen-from-14-companies/

[2] https[:]//blog.trendmicro[.]com/trendlabs-security-intelligence/us-local-government-services-targeted-by-new-magecart-credit-card-skimming-attack/

Access to linked reports require Falcon X Premium. Learn more | Manage subscription | Contact us

Copyright © 2020 CrowdStrike, Inc. All rights reserved.

CSWR-20025 CrowdStrike Intelligence Weekly Report: Week of 06/27/2020

From: intel-notifications@crowdstrike.com
To: christopher.moore@cookcountyil.gov, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>

Sent: July 3, 2020 3:27:37 PM CDT
Received: July 3, 2020 3:27:41 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.



CSWR-20025 CrowdStrike Intelligence Weekly Report: Week of 06/27/2020

On 22 July 2020, CrowdStrike Intelligence will host the Q2 Executive Briefing, an interactive session that will examine some of the notable activity and trends observed during April, May, and June. Briefing topics will include:

- Global Geopolitical Review
- Sector Threat Highlight: Telecommunications
- Update on Ransomware and Data Leaks
- INDRIK SPIDER: Post Indictment Changes
- WICKED PANDA: Attribution Challenges Posed with Cobalt Strike

Registration details for the Q2 Executive Briefing will be forthcoming soon.

Analysis Reveals CARBON SPIDER Use of REvil; JSS Loader Distribution Campaign Observed

Multiple instances of *REvil* (developed by PINCHY SPIDER) activity in conjunction with *Cobalt Strike* have been attributed with medium confidence by CrowdStrike Intelligence to CARBON SPIDER (CSA-200830). The activity suggests the adversary is monetizing access to networks without Point-of-Sale (PoS) systems by encrypting them with ransomware. The assessment is based on overlaps in tooling, infrastructure, and motivation. In particular, multiple connections were made through Cobalt Strike samples using the unique license identifier 452436291.

Separately, on 29 June 2020, CrowdStrike Intelligence identified a *Leo VBS* (CSA-191224) distribution campaign delivering *JSS Loader* (CSA-191197). While neither Leo VBS nor JSS Loader are unique to a particular adversary, it is likely this campaign was conducted by CARBON SPIDER. This assessment carries moderate confidence based on the combination of Tactics, Techniques, and Procedures (TTPs) and observed command-and-control (C2) infrastructure (CSA-200844).

Criminal Actor Installs Pharmaceutical-Themed Spam Pages on Compromised Web Server

On 25 June 2020, CrowdStrike Falcon OverWatch observed hands-on activity conducted by a criminal actor at a North America-based academic institution. The initial infection vector of the incident is unknown, but the hands-on-activity reveals interesting information about the actors TTPs (CSA-200834). Throughout 25 and 26 June, the criminal actor performed reconnaissance activity on the host by checking if their session was being debugged, locating the web root, and retrieving user account names. The actor proceeded to use `wget` to retrieve a ZIP archive from a remote location and decompressed the archive into the web root. The ZIP archive was over 500MB in size and contained more than 30,000 pharmaceutical-themed web pages advertising various medications available for online purchase without a prescription.

Reportedly New Ransom X Ransomware is Identified as Defray777

On 26 June 2020, security researchers published a report stating that a new ransomware named *Ransom X* had been used in an operation against a U.S.-based government transportation department. CrowdStrike Intelligence has obtained and analyzed samples of the reportedly new ransomware and has identified the family as the existing *Defray777* (CSA-200835).

Though security researchers use the name Defray777 to refer to this ransomware, the internal binary name set at compile time—`ransom.exx`—led to the name Ransom X. The new sample displays an updated ransom note format. Previously observed Defray777 ransom notes included an alternate contact method using BitMessage; however, this is no longer present in the new ransom note. The updated note includes updated instructions for the victim; however, the instruction to "contact someone from IT department" remains the same as in previous ransom notes.

New Ragnar Locker Victim Post Provides Insight to TTPs; Indications of Collaborations Between BGH Operators

A recent post by VIKING SPIDER on their dedicated leak site (DLS) detailing a new victim has provided insight to the operator's TTPs (CSA-200822). The post alludes to the actors exploiting vulnerabilities to secure initial access and moving laterally through the network after successfully elevating permissions to "Domain admin" level. Although the exact vulnerabilities exploited are unconfirmed, the information provides important insights to VIKING SPIDER's modus operandi.

There is increasing evidence of a collaboration or business relationship between VIKING SPIDER and the big game hunting (BGH) operators TWISTED SPIDER. Earlier in June, the two adversaries hosted victim information from each other's operations on their DLSs (CSA-200745). Both have reiterated their intent to refrain from targeting healthcare entities during the current pandemic, and both draw attention to their victims' security issues. This collaborative activity is unique in the current BGH threat landscape, with Ransomware-as-a-Service (RaaS) and affiliate programs the more commonly observed business arrangement.

Spam Campaign Mimicking Italian Revenue Agency Distributes Gozi ISFB

An Italian-language spam campaign involving emails mimicking the Italian Revenue Agency was observed on 29 June 2020 distributing the *Gozi ISFB* banking trojan (CSA-200842). The emails included Excel 4.0 macro documents, and referenced two articles of Italian legislation regarding tax refunds—the timing of the campaign was highly likely intended to coincide with Italy's annual tax deadline of 30 June. Phishing campaigns involving Excel 4.0 macro documents have become increasingly popular during 2020 (CSA-200461). In contrast to typical macro documents, which contain Visual Basic for Applications (VBA) macros, these documents use Excel 4.0 macros that predate VBA macros. It is likely adversaries are using Excel 4.0 macro documents to evade email and host-based security tools that are likely optimized to detect and prevent embedded VBA macros.

DanaBot Sub-Botnet 4 Distributing Avaddon Ransomware

SCULLY SPIDER's *DanaBot* sub-botnet 4 was observed by CrowdStrike Intelligence distributing *Avaddon* ransomware between 22 and 30 June 2020 (CSA-200846). This is the first instance of the sub-botnet delivering this ransomware variant—previous payloads delivered by sub-botnet 4 include WIZARD SPIDER's *Trickbot*, SMOKY SPIDER's *SmokeBot*, and various information stealers and remote administration tools (RATs).

Avaddon has previously been distributed in spam campaigns, including one campaign in June 2020 involving the *Phorpiex* malware targeting Japanese email addresses (CSA-200752). This Avaddon campaign was seemingly opportunistic, with no explicit sector or geographic focus identified.

INDRIK SPIDER's WastedLocker Continues to Grow Victim Base; BGH Operators Continue to Add Victim Details to DLS

INDRIK SPIDER has continued to target organizations primarily in the UK and North America using their new ransomware variant *WastedLocker* (CSA-200824). CrowdStrike Intelligence sensitive source reporting has confirmed 22 victims to date, with the manufacturing sector the most heavily targeted. Despite the naming of two key members of INDRIK SPIDER in unsealed indictments and others in financial sanctions, the group has continued to show resilience in their campaigns. *BitPaymer* operations have not been observed since mid-March 2020, and distribution of *Dridex* was last observed in late March 2020 (CSA-200403). The development and use of WastedLocker is likely intended to distance INDRIK SPIDER from their previous Dridex and BitPaymer operations—though similarities between BitPaymer and WastedLocker suggest such separation has not been fully achieved.

Alongside the identification of new WastedLocker victims, several other BGH operators added details of their victims to their associated DLS this week (see Figure 1).

Figure 1. BGH Ransomware Victims by Sector and Country (26 June to 2 July 2020)

Commodity Malware Updates and Underground Forum Activity; Stolen Datasets Advertised for Sale

Several updates, new releases, and advertisements were identified by CrowdStrike Intelligence within the past week on various criminal and underground forums for commodity malware variants (see summary in Table 1).

DATE	MALWARE	DETAILS
24 June 2020	Taurus Project Stealer	Update to newly released v1.4 • New panel includes loader statistics • Filter added for file grabber function • Wasabi and Daedalus collection added • Domain Detect redesigned
24 June 2020	Raccoon Stealer	Updates made to two versions: • Minor fixes and improvements to v1.5.12 • Added Chromium-based Microsoft Edge browser support for v1.5.13 • Bug fixed affecting auto-encryption in v1.5.13 • Downtime planned between 1 and 4 July 2020 for back-end update
25 June 2020	Buer Loader	Updates for v1.3.7 • Runtime cleaning • Added a loader directory for Windows Defender exceptions • Updated anti-virus
26 June 2020	Avaddon Ransomware	Updates to the build, including • Minor improvements and bug fixes • Panel access updated Ongoing recruitment for “networkers” Vendor urged customers to update to the latest version

26 June 2020	Triumph Loader	Update to v1.2.1 • Small update to the boot-loader • General improvements to the loader
29 June 2020	Amadey Loader	Update to v1.90 • File upload algorithm redesigned, and number of attempts to contact command-and-control (C2) server increased to 5 • Loader will reattempt at later date if target server is busy
29 June 2020	Oski Stealer	Update to v1.9.1, whereby helper DLLs downloaded from C2 are now obfuscated

Table 1. Commodity Malware Updates and Adverts

Also identified by CrowdStrike Intelligence sensitive sources are advertisements for various stolen datasets. These advertisements provide a snapshot of the type of information available to purchase or acquire from eCrime adversaries that can be used to perform phishing attacks or other fraudulent activity.

- A user on an underground forum known for database dumps and leaks recently shared a link to a dataset sourced from an Indian e-commerce platform. The data included personally identifiable information (PII) and contact details, including telephone numbers and postal addresses.
- On 26 June 2020, an Iranian eCrime actor advertised for sale the business credit card details for a U.S.-based commercial real estate company. The details were priced at $120 USD.
- A user with a proven track record of selling stolen government and academia-related databases advertised in June 2020 the sale of a database allegedly sourced from the Saudi Ministry of Interior. The data includes passport details, user records, and some travel-related information. The dataset is priced at $1,000 USD.

The Operators of Joker's Stash and Brian's Club Release Multiple Offerings of Compromised Payment Card Information with PII

The operators of Joker's Stash card shop released one offering from their three recent major breaches this week, BIGBADABOOM-III-US-part57. CrowdStrike Intelligence expects the weekly release of compromised payment card data from the NEW WORLD ORDER, BIGBADABOOM-III, and NIRVANA (releases advertised as LOTUS) breaches to continue, based on the historical activity of Joker's Stash card shop. Additionally, the operators of Joker's Stash released four offerings of compromised payment card data that contained personally PII from the U.S., EU, and other unspecified regions of the world. The abbreviation VBV in the offering highly likely indicates that it contains additional information to successfully bypass or complete Verified by Visa (VBV) fraud protection.

DATE	RELEASE NAME	REGION	NO. OF CARDS
27 June 2020	BIGELEPHANT-FULLINFO-	U.S./EU/World	10,000

	DOB-VBV		
29 June 2020	PINEAPPLE-FULLINFO-DOB-VBV	U.S./EU/World	15,000
30 June 2020	BEAUTIFULLIFE-FULLINFO-DOB-VBV	U.S./EU/World	15,000
1 July 2020	CULTURALSHOCK-FULLINFO-MIX	U.S./EU/World	1,000
1 July 2020	BIGBADABOOM-III-US-part57	U.S.	

Table 2. Recent Joker's Stash Card Shop Releases for 25 June - 2 July 2020

From 25 June to 2 July 2020, CrowdStrike Intelligence sources observed the card shop Brian's Club post five releases of compromised payment card information containing PII and included the cardholder's date of birth (DOB) and Social Security number (SSN).

DATE	RELEASE NAME	REGION	PII
25 June 2020	0625_US_IP_SSN	U.S.	DOB, SSN
26 June 2020	0626_US_IP_SSN	U.S.	DOB, SSN
27 June 2020	0627_US_IP_SSN	U.S.	DOB, SSN
28 June 2020	0628_US_IP_SSN	U.S.	DOB, SSN
29 June 2020	0629_US_IP_SSN	U.S.	DOB, SSN

Table 3. Brian's Club PII Offerings for 25 June- 2 July 2020

TARGETED INTRUSION

WICKED PANDA Deploys RouterGod Malware in Targeted Attacks Against Southeast Asian Entities

As part of ongoing targeted activity against Southeast Asian entities, CrowdStrike Falcon OverWatch detected the deployment of novel malware, named *RouterGod*, at an entity associated with the aviation industry in Hong Kong. This malware has likely been used to target entities in Hong-Kong, Macau, and Taiwan with the actor also deploying additional tools such as *Cobalt Strike*, *DarkShell*, and *Proxip* as part of the same campaign. The Proxip and Cobalt Strike samples are configured to use subdomains of `livehost[.]live`, a domain used by WICKED PANDA as part of ShadowPad activity targeting Hong Kong-based universities in 2019 (CSA-200151). Because of the re-use of this low prevalence domain, continued targeting of Southeast Asian entities as well as the deployment of Proxip and Cobalt Strike in tandem, CrowdStrike Intelligence currently attributes this activity to WICKED PANDA with high confidence.

The name RouterGod is used internally by the malware developers, likely due to the ability of the malware to route encrypted command packets between infected hosts. RouterGod is a .NET executable that can be used to execute arbitrary scripts as well as establish sessions with other infected hosts. Multiple instances of the malware can be used in a chain to deliver implant tasking to specific endpoints within victim networks. Additional technical analysis is available in CSA-200848.

Novel Malware Families Loosely Linked to China Identified

This week, CrowdStrike Intelligence released initial analytic findings on newly identified malware. Both malware families were used in operations consistent with Chinese state-nexus activity:

- In June 2020, CrowdStrike Falcon OverWatch observed an unknown adversary deploy novel malware as part of an attempted compromise at a Southeast Asian IT services provider. The deployed malware uses a legitimate antivirus product executable to gain execution via dynamic link library (DLL) search-order hijacking in order to execute a malicious loader DLL that, in turn, decrypts and loads an associated payload file. Additional activity observed included the execution of a Cobalt Strike stager executable that was used to download an additional payload as well as PowerShell commands used to contact unknown infrastructure. See CSA-200849 for more information.

- Also in June 2020, CrowdStrike Falcon OverWatch identified two closely related incidents at an East Asian multinational pharmaceutical company. Both instances featured a previously unseen implant linked to activity CrowdStrike has assessed as consistent with Chinese state interests. For this activity, legitimate VirtualBox executables were used to host malicious DLLs that in turn load and deobfuscate the malicious payloads. See CSA-200833 for more information.

IMPERIAL KITTEN Continues Operations Against Probable Saudi Arabian Technology Organizations with New FireBAK Variant

CrowdStrike Intelligence has identified continued activity from the Iranian state-nexus IMPERIAL KITTEN adversary throughout the first half of 2020. The activity consisted of the apparent continued development of its *FireBAK* implant, with new variants written in PowerShell and Visual Basic Script (VBS). Additional deployment of the adversary's custom *LaZagne* variant were identified in late June 2020. Additional data suggests that current IMPERIAL KITTEN operations likely focus on technology-related organizations in Saudi Arabia. For more information, see CSA-200843.

New LampCarrier Cluster Activity and Infrastructure Identified

CrowdStrike Intelligence has discovered previously unidentified activity attributed to the LampCarrier cluster including Golang-based malware, a Microsoft Office document containing a malicious macro, and previously unidentified infrastructure. Previously observed LampCarrier activity did not include malware as a significant part of its toolset, as the actor preferred to rely on living-off-the land techniques. The discovery of new malware and malicious documents indicates LampCarrier is evolving its TTPs, particularly in how it establishes persistence on victim networks. Additional information and Indicators of Compromise (IOCs) are available in CSA-200831.

HACKTIVISM

MENA Hacktivists Engage in Doxxing and Defacement Activity

On 28 June 2020, hacktivist group *Oman Hackers* claimed to have doxxed more than 20 individuals they believe responsible for managing social media accounts conducting information operations against Omani interests. The vast majority of the purportedly doxxed individuals were Emirati,

although some citizens of other countries in the Middle East and North Africa (MENA) were also identified. The Oman Hackers group claim to have obtained this information by compromising a fake account managed by one of the doxxed individuals and then identifying additional accounts involved in coordinating inauthentic behavior. In particular, the Oman Hackers group focused its doxxing efforts on three individuals whom the group believes to have ties to various Emirati government and security institutions as well as some legal and media organizations. The Oman Hackers group is currently highly active, continuing to claim that an organized conspiracy is harming the Omani government, its regime, and the country's relations with neighboring countries. For more information, see CSA-200836.

Throughout June 2020, hacktivists operating under the moniker *Moroccan Revolution* have reported more than 1200 notifications to the website defacement archive Zone-H. While the group has been active since at least 2015, June 2020 marked a significant increase in defacement claims. Only two of the defacements listed in Zone-H records noted defacements of government websites in June, both of which were in Vietnam. The defacement activity is very likely opportunistic in nature rather than specifically targeted, due to the large number of defacements with no clear geographic or sector targeting theme. While CrowdStrike Intelligence has not independently attributed the geographic origins of most members claiming association with the group, Moroccan Revolution likely consists broadly of North African hacktivists or individuals sympathetic to issues in the region. Additional information is available in CSA-200828.

Fallout from BlueLeaks Release of Sensitive U.S. Law Enforcement Data

On 19 June 2020, hacktivist-journalist entity Distributed Denial of Secrets (*DDOS*) released 269 GB of materials belonging to hundreds of law enforcement agencies across the U.S., naming the collection BlueLeaks (CSA-200801). The release coincided with protests against U.S. law enforcement agencies after the killing of George FLOYD on 25 May and follows similar protests against law enforcement in Latin America (LATAM). Journalist and operator of DDOS Emma BEST—known to work closely with sophisticated hacktivist MOLOTOV JACKAL and has an established track record of publishing materials in the advancement of anti-capitalist and other ideologies (CSA-200663)—made an open call for breaches of U.S. police forces, requesting that hacktivists leak any exfiltrated data to DDOS (CSA-200697). BlueLeaks leveraged at least three simultaneous means of access and distribution: a searchable web portal, a Tor mirror for the portal, and a downloadable Torrent file for the full collection; recent leaks of sensitive law enforcement data in LATAM were published in a similar manner, with a user-friendly GUI enabling easier digestion of the data (CSIT-19233).

Among the BlueLeaks data were sensitive documents belonging to the Maine Information and Analysis Center (MIAC). Internal MIAC communication was allegedly not compromised but results of requests for information (RFIs) were exposed, including personally identifiable information (PII) of subjects and victims as well as information regarding ongoing investigations in Maine. It was also revealed that MIAC has been closely tracking Black Lives Matter (BLM) events and advocacy groups (CSDR-20075).

Hacktivist Campaign Protests Colombian Military Scandal

On 26 June 2020, hacktivist group *Anonymous Colombia* posted an English-language video announcing a campaign to protest acts of extreme violence seven Colombian soldiers committed against indigenous children. The group claimed credit for a DDoS attack and website defacement against two separate websites belonging to former Colombian president and current Senator Álvaro URIBE. A separate hacktivist group known as *Anonym0us China* backed the campaign, claiming responsibility for a DDoS attack of the Colombian Army's English and Spanish-language websites. This operation was the second Anonymous-linked #OpColombia campaign announced that week;

there has been no observed overlap between the actors claiming the activities, highlighting the decentralized nature of the Anonymous movement. For more information, see CSA-200839.

Iranian Hacktivists Target Israeli, U.S. Based Entities

Iranian hacktivist group *Death Squads* claimed credit for a DDoS attack against the domains of an Israeli domain registrar and a U.S.-based bank. As the veracity and credibility of these attacks cannot be confirmed, the attack and associated denial of service were likely limited in duration and effect. Death Squads' latest claims represent a departure from past efforts and are assessed to likely be geopolitically motivated due to the group's nationalistic outlook and the backgrounds of its core membership. This effort is likely of low sophistication and representative of a singular hacktivist effort rather than part of a wider campaign. See CSA-200837 for more information.

The timing of the claim also coincides with additional (though apparently unrelated) attacks claimed by Iranian hacktivist groups *Vortex Security Team* and *Unidentified Security Team* against Israel. Specifically, the groups claimed what appear to be two distinct alleged intrusions: one targeting an Israeli gas company's server and the other against an unknown entity. The server is assessed to likely have been identified via exposed services or port-scanning activity; the propensity of hacktivists to conflate publicly available information with data breaches suggests there are even chances the extent of the intrusion was either exaggerated or extremely limited in scale. The hacktivist groups claim that a 27 June explosion near an Iranian military base on 24 June was a result of an Israeli cyberattack, and the groups took retaliatory action in response. For further reading, see CSA-200840.

DATA EXPOSURE & BREACHES

Threat Actor Reportedly Selling Data Stolen From 14 Companies

A threat actor is reportedly selling databases stolen from 14 different companies on an underground forum, according to media reports.[1] Stolen data varies per company, though all breaches reportedly include usernames and hashed passwords. The threat actor is selling the databases at varying prices, ranging from $100 to $1,100 USD. The companies were all allegedly breached in 2020, though the exact dates of compromise, if true, remains unknown. Of the fourteen companies, four companies have previously reported breaches. It is currently unclear if the stolen databases from those four companies are connected to the previously reported breaches.

Eight U.S. Cities Reportedly Impacted by Click2Gov Breaches

The local governments of eight U.S.-based cities discovered a JavaScript (JS) skimmer had been injected into the payment portals of their Click2Gov sites.[2] The eight cities were located across three U.S. states. Industry researchers disclosed two different exfiltration servers that hosted the JS skimmer; one server was used for three sites and one used for the remaining five sites. The JS skimmer was designed to collect payment card information, including card number, expiration date, and CVV, as well as names and physical addresses. Media reports speculate that these compromises are the result of a threat group leveraging *Magecart* tactics. However, CrowdStrike Intelligence does not currently attribute this activity to a known adversary at this time.

Recent Reporting

CSIT-20100 Analysis of TRACER KITTEN DNSDAT Malware Targeting the Middle Eastern Telecommunications Sector

This Tipper provides technical analysis of the *DNSDAT* malware in use by the Iranian actor TRACER KITTEN.

CSMR-20005 CrowdStrike Intelligence Monthly Report - May 2020

This report provides significant analytic findings from May 2020, including trends observed in targeted intrusion, eCrime, and hacktivist operations.

[1] https[:]//www.bleepingcomputer[.]com/news/security/seller-floods-hacker-forum-with-data-stolen-from-14-companies/

[2] https[:]//blog.trendmicro[.]com/trendlabs-security-intelligence/us-local-government-services-targeted-by-new-magecart-credit-card-skimming-attack/

Access to linked reports require Falcon X Premium. Learn more | Manage subscription | Contact us

Copyright © 2020 CrowdStrike, Inc. All rights reserved.

CSWR-20025 CrowdStrike Intelligence Weekly Report: Week of 06/27/2020

From: intel-notifications@crowdstrike.com
To: patrick.kelly@cookcountyil.gov, Patrick Kelly (Sheriff) <Patrick.Kelly@cookcountyil.gov>

Sent: July 3, 2020 3:33:02 PM CDT
Received: July 3, 2020 3:33:07 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.



CSWR-20025 CrowdStrike Intelligence Weekly Report: Week of 06/27/2020

On 22 July 2020, CrowdStrike Intelligence will host the Q2 Executive Briefing, an interactive session that will examine some of the notable activity and trends observed during April, May, and June. Briefing topics will include:

- Global Geopolitical Review
- Sector Threat Highlight: Telecommunications
- Update on Ransomware and Data Leaks
- INDRIK SPIDER: Post Indictment Changes
- WICKED PANDA: Attribution Challenges Posed with Cobalt Strike

Registration details for the Q2 Executive Briefing will be forthcoming soon.

Analysis Reveals CARBON SPIDER Use of REvil; JSS Loader Distribution Campaign Observed

Multiple instances of *REvil* (developed by PINCHY SPIDER) activity in conjunction with *Cobalt Strike* have been attributed with medium confidence by CrowdStrike Intelligence to CARBON SPIDER (CSA-200830). The activity suggests the adversary is monetizing access to networks without Point-of-Sale (PoS) systems by encrypting them with ransomware. The assessment is based on overlaps in tooling, infrastructure, and motivation. In particular, multiple connections were made through Cobalt Strike samples using the unique license identifier 452436291.

Separately, on 29 June 2020, CrowdStrike Intelligence identified a *Leo VBS* (CSA-191224) distribution campaign delivering *JSS Loader* (CSA-191197). While neither Leo VBS nor JSS Loader are unique to a particular adversary, it is likely this campaign was conducted by CARBON SPIDER. This assessment carries moderate confidence based on the combination of Tactics, Techniques, and Procedures (TTPs) and observed command-and-control (C2) infrastructure (CSA-200844).

Criminal Actor Installs Pharmaceutical-Themed Spam Pages on Compromised Web Server

On 25 June 2020, CrowdStrike Falcon OverWatch observed hands-on activity conducted by a criminal actor at a North America-based academic institution. The initial infection vector of the incident is unknown, but the hands-on-activity reveals interesting information about the actors TTPs (CSA-200834). Throughout 25 and 26 June, the criminal actor performed reconnaissance activity on the host by checking if their session was being debugged, locating the web root, and retrieving user account names. The actor proceeded to use `wget` to retrieve a ZIP archive from a remote location and decompressed the archive into the web root. The ZIP archive was over 500MB in size and contained more than 30,000 pharmaceutical-themed web pages advertising various medications available for online purchase without a prescription.

Reportedly New Ransom X Ransomware is Identified as Defray777

On 26 June 2020, security researchers published a report stating that a new ransomware named *Ransom X* had been used in an operation against a U.S.-based government transportation department. CrowdStrike Intelligence has obtained and analyzed samples of the reportedly new ransomware and has identified the family as the existing *Defray777* (CSA-200835).

Though security researchers use the name Defray777 to refer to this ransomware, the internal binary name set at compile time—`ransom.exx`—led to the name Ransom X. The new sample displays an updated ransom note format. Previously observed Defray777 ransom notes included an alternate contact method using BitMessage; however, this is no longer present in the new ransom note. The updated note includes updated instructions for the victim; however, the instruction to "contact someone from IT department" remains the same as in previous ransom notes.

New Ragnar Locker Victim Post Provides Insight to TTPs; Indications of Collaborations Between BGH Operators

A recent post by VIKING SPIDER on their dedicated leak site (DLS) detailing a new victim has provided insight to the operator's TTPs (CSA-200822). The post alludes to the actors exploiting vulnerabilities to secure initial access and moving laterally through the network after successfully elevating permissions to "Domain admin" level. Although the exact vulnerabilities exploited are unconfirmed, the information provides important insights to VIKING SPIDER's modus operandi.

There is increasing evidence of a collaboration or business relationship between VIKING SPIDER and the big game hunting (BGH) operators TWISTED SPIDER. Earlier in June, the two adversaries hosted victim information from each other's operations on their DLSs (CSA-200745). Both have reiterated their intent to refrain from targeting healthcare entities during the current pandemic, and both draw attention to their victims' security issues. This collaborative activity is unique in the current BGH threat landscape, with Ransomware-as-a-Service (RaaS) and affiliate programs the more commonly observed business arrangement.

Spam Campaign Mimicking Italian Revenue Agency Distributes Gozi ISFB

An Italian-language spam campaign involving emails mimicking the Italian Revenue Agency was observed on 29 June 2020 distributing the *Gozi ISFB* banking trojan (CSA-200842). The emails included Excel 4.0 macro documents, and referenced two articles of Italian legislation regarding tax refunds—the timing of the campaign was highly likely intended to coincide with Italy's annual tax deadline of 30 June. Phishing campaigns involving Excel 4.0 macro documents have become increasingly popular during 2020 (CSA-200461). In contrast to typical macro documents, which contain Visual Basic for Applications (VBA) macros, these documents use Excel 4.0 macros that predate VBA macros. It is likely adversaries are using Excel 4.0 macro documents to evade email and host-based security tools that are likely optimized to detect and prevent embedded VBA macros.

DanaBot Sub-Botnet 4 Distributing Avaddon Ransomware

SCULLY SPIDER's *DanaBot* sub-botnet 4 was observed by CrowdStrike Intelligence distributing *Avaddon* ransomware between 22 and 30 June 2020 (CSA-200846). This is the first instance of the sub-botnet delivering this ransomware variant—previous payloads delivered by sub-botnet 4 include WIZARD SPIDER's *Trickbot*, SMOKY SPIDER's *SmokeBot*, and various information stealers and remote administration tools (RATs).

Avaddon has previously been distributed in spam campaigns, including one campaign in June 2020 involving the *Phorpiex* malware targeting Japanese email addresses (CSA-200752). This Avaddon campaign was seemingly opportunistic, with no explicit sector or geographic focus identified.

INDRIK SPIDER's WastedLocker Continues to Grow Victim Base; BGH Operators Continue to Add Victim Details to DLS

INDRIK SPIDER has continued to target organizations primarily in the UK and North America using their new ransomware variant *WastedLocker* (CSA-200824). CrowdStrike Intelligence sensitive source reporting has confirmed 22 victims to date, with the manufacturing sector the most heavily targeted. Despite the naming of two key members of INDRIK SPIDER in unsealed indictments and others in financial sanctions, the group has continued to show resilience in their campaigns. *BitPaymer* operations have not been observed since mid-March 2020, and distribution of *Dridex* was last observed in late March 2020 (CSA-200403). The development and use of WastedLocker is likely intended to distance INDRIK SPIDER from their previous Dridex and BitPaymer operations—though similarities between BitPaymer and WastedLocker suggest such separation has not been fully achieved.

Alongside the identification of new WastedLocker victims, several other BGH operators added details of their victims to their associated DLS this week (see Figure 1).

Figure 1. BGH Ransomware Victims by Sector and Country (26 June to 2 July 2020)

Commodity Malware Updates and Underground Forum Activity; Stolen Datasets Advertised for Sale

Several updates, new releases, and advertisements were identified by CrowdStrike Intelligence within the past week on various criminal and underground forums for commodity malware variants (see summary in Table 1).

DATE	MALWARE	DETAILS
24 June 2020	Taurus Project Stealer	Update to newly released v1.4 • New panel includes loader statistics • Filter added for file grabber function • Wasabi and Daedalus collection added • Domain Detect redesigned
24 June 2020	Raccoon Stealer	Updates made to two versions: • Minor fixes and improvements to v1.5.12 • Added Chromium-based Microsoft Edge browser support for v1.5.13 • Bug fixed affecting auto-encryption in v1.5.13 • Downtime planned between 1 and 4 July 2020 for back-end update
25 June 2020	Buer Loader	Updates for v1.3.7 • Runtime cleaning • Added a loader directory for Windows Defender exceptions • Updated anti-virus
26 June 2020	Avaddon Ransomware	Updates to the build, including • Minor improvements and bug fixes • Panel access updated Ongoing recruitment for “networkers” Vendor urged customers to update to the latest version

26 June 2020	Triumph Loader	Update to v1.2.1 • Small update to the boot-loader • General improvements to the loader
29 June 2020	Amadey Loader	Update to v1.90 • File upload algorithm redesigned, and number of attempts to contact command-and-control (C2) server increased to 5 • Loader will reattempt at later date if target server is busy
29 June 2020	Oski Stealer	Update to v1.9.1, whereby helper DLLs downloaded from C2 are now obfuscated

Table 1. Commodity Malware Updates and Adverts

Also identified by CrowdStrike Intelligence sensitive sources are advertisements for various stolen datasets. These advertisements provide a snapshot of the type of information available to purchase or acquire from eCrime adversaries that can be used to perform phishing attacks or other fraudulent activity.

- A user on an underground forum known for database dumps and leaks recently shared a link to a dataset sourced from an Indian e-commerce platform. The data included personally identifiable information (PII) and contact details, including telephone numbers and postal addresses.
- On 26 June 2020, an Iranian eCrime actor advertised for sale the business credit card details for a U.S.-based commercial real estate company. The details were priced at $120 USD.
- A user with a proven track record of selling stolen government and academia-related databases advertised in June 2020 the sale of a database allegedly sourced from the Saudi Ministry of Interior. The data includes passport details, user records, and some travel-related information. The dataset is priced at $1,000 USD.

The Operators of Joker's Stash and Brian's Club Release Multiple Offerings of Compromised Payment Card Information with PII

The operators of Joker's Stash card shop released one offering from their three recent major breaches this week, BIGBADABOOM-III-US-part57. CrowdStrike Intelligence expects the weekly release of compromised payment card data from the NEW WORLD ORDER, BIGBADABOOM-III, and NIRVANA (releases advertised as LOTUS) breaches to continue, based on the historical activity of Joker's Stash card shop. Additionally, the operators of Joker's Stash released four offerings of compromised payment card data that contained personally PII from the U.S., EU, and other unspecified regions of the world. The abbreviation VBV in the offering highly likely indicates that it contains additional information to successfully bypass or complete Verified by Visa (VBV) fraud protection.

DATE	RELEASE NAME	REGION	NO. OF CARDS
27 June 2020	BIGELEPHANT-FULLINFO-	U.S./EU/World	10,000

	DOB-VBV		
29 June 2020	PINEAPPLE-FULLINFO-DOB-VBV	U.S./EU/World	15,000
30 June 2020	BEAUTIFULLIFE-FULLINFO-DOB-VBV	U.S./EU/World	15,000
1 July 2020	CULTURALSHOCK-FULLINFO-MIX	U.S./EU/World	1,000
1 July 2020	BIGBADABOOM-III-US-part57	U.S.	

Table 2. Recent Joker's Stash Card Shop Releases for 25 June - 2 July 2020

From 25 June to 2 July 2020, CrowdStrike Intelligence sources observed the card shop Brian's Club post five releases of compromised payment card information containing PII and included the cardholder's date of birth (DOB) and Social Security number (SSN).

DATE	RELEASE NAME	REGION	PII
25 June 2020	0625_US_IP_SSN	U.S.	DOB, SSN
26 June 2020	0626_US_IP_SSN	U.S.	DOB, SSN
27 June 2020	0627_US_IP_SSN	U.S.	DOB, SSN
28 June 2020	0628_US_IP_SSN	U.S.	DOB, SSN
29 June 2020	0629_US_IP_SSN	U.S.	DOB, SSN

Table 3. Brian's Club PII Offerings for 25 June- 2 July 2020

TARGETED INTRUSION

WICKED PANDA Deploys RouterGod Malware in Targeted Attacks Against Southeast Asian Entities

As part of ongoing targeted activity against Southeast Asian entities, CrowdStrike Falcon OverWatch detected the deployment of novel malware, named *RouterGod*, at an entity associated with the aviation industry in Hong Kong. This malware has likely been used to target entities in Hong-Kong, Macau, and Taiwan with the actor also deploying additional tools such as *Cobalt Strike*, *DarkShell*, and *Proxip* as part of the same campaign. The Proxip and Cobalt Strike samples are configured to use subdomains of `livehost[.]live`, a domain used by WICKED PANDA as part of ShadowPad activity targeting Hong Kong-based universities in 2019 (CSA-200151). Because of the re-use of this low prevalence domain, continued targeting of Southeast Asian entities as well as the deployment of Proxip and Cobalt Strike in tandem, CrowdStrike Intelligence currently attributes this activity to WICKED PANDA with high confidence.

The name RouterGod is used internally by the malware developers, likely due to the ability of the malware to route encrypted command packets between infected hosts. RouterGod is a .NET executable that can be used to execute arbitrary scripts as well as establish sessions with other infected hosts. Multiple instances of the malware can be used in a chain to deliver implant tasking to specific endpoints within victim networks. Additional technical analysis is available in CSA-200848.

Novel Malware Families Loosely Linked to China Identified

This week, CrowdStrike Intelligence released initial analytic findings on newly identified malware. Both malware families were used in operations consistent with Chinese state-nexus activity:

- In June 2020, CrowdStrike Falcon OverWatch observed an unknown adversary deploy novel malware as part of an attempted compromise at a Southeast Asian IT services provider. The deployed malware uses a legitimate antivirus product executable to gain execution via dynamic link library (DLL) search-order hijacking in order to execute a malicious loader DLL that, in turn, decrypts and loads an associated payload file. Additional activity observed included the execution of a Cobalt Strike stager executable that was used to download an additional payload as well as PowerShell commands used to contact unknown infrastructure. See CSA-200849 for more information.

- Also in June 2020, CrowdStrike Falcon OverWatch identified two closely related incidents at an East Asian multinational pharmaceutical company. Both instances featured a previously unseen implant linked to activity CrowdStrike has assessed as consistent with Chinese state interests. For this activity, legitimate VirtualBox executables were used to host malicious DLLs that in turn load and deobfuscate the malicious payloads. See CSA-200833 for more information.

IMPERIAL KITTEN Continues Operations Against Probable Saudi Arabian Technology Organizations with New FireBAK Variant

CrowdStrike Intelligence has identified continued activity from the Iranian state-nexus IMPERIAL KITTEN adversary throughout the first half of 2020. The activity consisted of the apparent continued development of its *FireBAK* implant, with new variants written in PowerShell and Visual Basic Script (VBS). Additional deployment of the adversary's custom *LaZagne* variant were identified in late June 2020. Additional data suggests that current IMPERIAL KITTEN operations likely focus on technology-related organizations in Saudi Arabia. For more information, see CSA-200843.

New LampCarrier Cluster Activity and Infrastructure Identified

CrowdStrike Intelligence has discovered previously unidentified activity attributed to the LampCarrier cluster including Golang-based malware, a Microsoft Office document containing a malicious macro, and previously unidentified infrastructure. Previously observed LampCarrier activity did not include malware as a significant part of its toolset, as the actor preferred to rely on living-off-the land techniques. The discovery of new malware and malicious documents indicates LampCarrier is evolving its TTPs, particularly in how it establishes persistence on victim networks. Additional information and Indicators of Compromise (IOCs) are available in CSA-200831.

HACKTIVISM

MENA Hacktivists Engage in Doxxing and Defacement Activity

On 28 June 2020, hacktivist group *Oman Hackers* claimed to have doxxed more than 20 individuals they believe responsible for managing social media accounts conducting information operations against Omani interests. The vast majority of the purportedly doxxed individuals were Emirati,

although some citizens of other countries in the Middle East and North Africa (MENA) were also identified. The Oman Hackers group claim to have obtained this information by compromising a fake account managed by one of the doxxed individuals and then identifying additional accounts involved in coordinating inauthentic behavior. In particular, the Oman Hackers group focused its doxxing efforts on three individuals whom the group believes to have ties to various Emirati government and security institutions as well as some legal and media organizations. The Oman Hackers group is currently highly active, continuing to claim that an organized conspiracy is harming the Omani government, its regime, and the country's relations with neighboring countries. For more information, see CSA-200836.

Throughout June 2020, hacktivists operating under the moniker *Moroccan Revolution* have reported more than 1200 notifications to the website defacement archive Zone-H. While the group has been active since at least 2015, June 2020 marked a significant increase in defacement claims. Only two of the defacements listed in Zone-H records noted defacements of government websites in June, both of which were in Vietnam. The defacement activity is very likely opportunistic in nature rather than specifically targeted, due to the large number of defacements with no clear geographic or sector targeting theme. While CrowdStrike Intelligence has not independently attributed the geographic origins of most members claiming association with the group, Moroccan Revolution likely consists broadly of North African hacktivists or individuals sympathetic to issues in the region. Additional information is available in CSA-200828.

Fallout from BlueLeaks Release of Sensitive U.S. Law Enforcement Data

On 19 June 2020, hacktivist-journalist entity Distributed Denial of Secrets (*DDOS*) released 269 GB of materials belonging to hundreds of law enforcement agencies across the U.S., naming the collection BlueLeaks (CSA-200801). The release coincided with protests against U.S. law enforcement agencies after the killing of George FLOYD on 25 May and follows similar protests against law enforcement in Latin America (LATAM). Journalist and operator of DDOS Emma BEST—known to work closely with sophisticated hacktivist MOLOTOV JACKAL and has an established track record of publishing materials in the advancement of anti-capitalist and other ideologies (CSA-200663)—made an open call for breaches of U.S. police forces, requesting that hacktivists leak any exfiltrated data to DDOS (CSA-200697). BlueLeaks leveraged at least three simultaneous means of access and distribution: a searchable web portal, a Tor mirror for the portal, and a downloadable Torrent file for the full collection; recent leaks of sensitive law enforcement data in LATAM were published in a similar manner, with a user-friendly GUI enabling easier digestion of the data (CSIT-19233).

Among the BlueLeaks data were sensitive documents belonging to the Maine Information and Analysis Center (MIAC). Internal MIAC communication was allegedly not compromised but results of requests for information (RFIs) were exposed, including personally identifiable information (PII) of subjects and victims as well as information regarding ongoing investigations in Maine. It was also revealed that MIAC has been closely tracking Black Lives Matter (BLM) events and advocacy groups (CSDR-20075).

Hacktivist Campaign Protests Colombian Military Scandal

On 26 June 2020, hacktivist group *Anonymous Colombia* posted an English-language video announcing a campaign to protest acts of extreme violence seven Colombian soldiers committed against indigenous children. The group claimed credit for a DDoS attack and website defacement against two separate websites belonging to former Colombian president and current Senator Álvaro URIBE. A separate hacktivist group known as *Anonym0us China* backed the campaign, claiming responsibility for a DDoS attack of the Colombian Army's English and Spanish-language websites. This operation was the second Anonymous-linked #OpColombia campaign announced that week;

there has been no observed overlap between the actors claiming the activities, highlighting the decentralized nature of the Anonymous movement. For more information, see CSA-200839.

Iranian Hacktivists Target Israeli, U.S. Based Entities

Iranian hacktivist group *Death Squads* claimed credit for a DDoS attack against the domains of an Israeli domain registrar and a U.S.-based bank. As the veracity and credibility of these attacks cannot be confirmed, the attack and associated denial of service were likely limited in duration and effect. Death Squads' latest claims represent a departure from past efforts and are assessed to likely be geopolitically motivated due to the group's nationalistic outlook and the backgrounds of its core membership. This effort is likely of low sophistication and representative of a singular hacktivist effort rather than part of a wider campaign. See CSA-200837 for more information.

The timing of the claim also coincides with additional (though apparently unrelated) attacks claimed by Iranian hacktivist groups *Vortex Security Team* and *Unidentified Security Team* against Israel. Specifically, the groups claimed what appear to be two distinct alleged intrusions: one targeting an Israeli gas company's server and the other against an unknown entity. The server is assessed to likely have been identified via exposed services or port-scanning activity; the propensity of hacktivists to conflate publicly available information with data breaches suggests there are even chances the extent of the intrusion was either exaggerated or extremely limited in scale. The hacktivist groups claim that a 27 June explosion near an Iranian military base on 24 June was a result of an Israeli cyberattack, and the groups took retaliatory action in response. For further reading, see CSA-200840.

DATA EXPOSURE & BREACHES

Threat Actor Reportedly Selling Data Stolen From 14 Companies

A threat actor is reportedly selling databases stolen from 14 different companies on an underground forum, according to media reports.[1] Stolen data varies per company, though all breaches reportedly include usernames and hashed passwords. The threat actor is selling the databases at varying prices, ranging from $100 to $1,100 USD. The companies were all allegedly breached in 2020, though the exact dates of compromise, if true, remains unknown. Of the fourteen companies, four companies have previously reported breaches. It is currently unclear if the stolen databases from those four companies are connected to the previously reported breaches.

Eight U.S. Cities Reportedly Impacted by Click2Gov Breaches

The local governments of eight U.S.-based cities discovered a JavaScript (JS) skimmer had been injected into the payment portals of their Click2Gov sites.[2] The eight cities were located across three U.S. states. Industry researchers disclosed two different exfiltration servers that hosted the JS skimmer; one server was used for three sites and one used for the remaining five sites. The JS skimmer was designed to collect payment card information, including card number, expiration date, and CVV, as well as names and physical addresses. Media reports speculate that these compromises are the result of a threat group leveraging *Magecart* tactics. However, CrowdStrike Intelligence does not currently attribute this activity to a known adversary at this time.

Recent Reporting

CSIT-20100 Analysis of TRACER KITTEN DNSDAT Malware Targeting the Middle Eastern Telecommunications Sector

This Tipper provides technical analysis of the *DNSDAT* malware in use by the Iranian actor TRACER KITTEN.

CSMR-20005 CrowdStrike Intelligence Monthly Report - May 2020

This report provides significant analytic findings from May 2020, including trends observed in targeted intrusion, eCrime, and hacktivist operations.

[1] https[:]//www.bleepingcomputer[.]com/news/security/seller-floods-hacker-forum-with-data-stolen-from-14-companies/

[2] https[:]//blog.trendmicro[.]com/trendlabs-security-intelligence/us-local-government-services-targeted-by-new-magecart-credit-card-skimming-attack/

Access to linked reports require Falcon X Premium. Learn more | Manage subscription | Contact us

Copyright © 2020 CrowdStrike, Inc. All rights reserved.

CSWR-20025 CrowdStrike Intelligence Weekly Report: Week of 06/27/2020

To:	Patrick Kelly (Sheriff), Keith Morrison (Sheriff), Christopher Moore (Sheriff), Jonathan Springborn (Sheriff), Michael Aliperti, Ben Spear
Sent:	July 3, 2020 3:33:02 PM CDT
Received:	July 3, 2020 3:33:07 PM CDT

CSWR-20025 CrowdStrike Intelligence Weekly Report: Week of 06/27/2020

From: intel-notifications@crowdstrike.com
To: jonathan.springborn@cookcountyil.gov, Jonathan Springborn (Sheriff) <Jonathan.Springborn@cookcountyil.gov>

Sent: July 3, 2020 3:33:19 PM CDT
Received: July 3, 2020 3:33:24 PM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.



CSWR-20025 CrowdStrike Intelligence Weekly Report: Week of 06/27/2020

On 22 July 2020, CrowdStrike Intelligence will host the Q2 Executive Briefing, an interactive session that will examine some of the notable activity and trends observed during April, May, and June. Briefing topics will include:

- Global Geopolitical Review
- Sector Threat Highlight: Telecommunications
- Update on Ransomware and Data Leaks
- INDRIK SPIDER: Post Indictment Changes
- WICKED PANDA: Attribution Challenges Posed with Cobalt Strike

Registration details for the Q2 Executive Briefing will be forthcoming soon.

Analysis Reveals CARBON SPIDER Use of REvil; JSS Loader Distribution Campaign Observed

Multiple instances of *REvil* (developed by PINCHY SPIDER) activity in conjunction with *Cobalt Strike* have been attributed with medium confidence by CrowdStrike Intelligence to CARBON SPIDER (CSA-200830). The activity suggests the adversary is monetizing access to networks without Point-of-Sale (PoS) systems by encrypting them with ransomware. The assessment is based on overlaps in tooling, infrastructure, and motivation. In particular, multiple connections were made through Cobalt Strike samples using the unique license identifier 452436291.

Separately, on 29 June 2020, CrowdStrike Intelligence identified a *Leo VBS* (CSA-191224) distribution campaign delivering *JSS Loader* (CSA-191197). While neither Leo VBS nor JSS Loader are unique to a particular adversary, it is likely this campaign was conducted by CARBON SPIDER. This assessment carries moderate confidence based on the combination of Tactics, Techniques, and Procedures (TTPs) and observed command-and-control (C2) infrastructure (CSA-200844).

Criminal Actor Installs Pharmaceutical-Themed Spam Pages on Compromised Web Server

On 25 June 2020, CrowdStrike Falcon OverWatch observed hands-on activity conducted by a criminal actor at a North America-based academic institution. The initial infection vector of the incident is unknown, but the hands-on-activity reveals interesting information about the actors TTPs (CSA-200834). Throughout 25 and 26 June, the criminal actor performed reconnaissance activity on the host by checking if their session was being debugged, locating the web root, and retrieving user account names. The actor proceeded to use `wget` to retrieve a ZIP archive from a remote location and decompressed the archive into the web root. The ZIP archive was over 500MB in size and contained more than 30,000 pharmaceutical-themed web pages advertising various medications available for online purchase without a prescription.

Reportedly New Ransom X Ransomware is Identified as Defray777

On 26 June 2020, security researchers published a report stating that a new ransomware named *Ransom X* had been used in an operation against a U.S.-based government transportation department. CrowdStrike Intelligence has obtained and analyzed samples of the reportedly new ransomware and has identified the family as the existing *Defray777* (CSA-200835).

Though security researchers use the name Defray777 to refer to this ransomware, the internal binary name set at compile time—`ransom.exx`—led to the name Ransom X. The new sample displays an updated ransom note format. Previously observed Defray777 ransom notes included an alternate contact method using BitMessage; however, this is no longer present in the new ransom note. The updated note includes updated instructions for the victim; however, the instruction to "contact someone from IT department" remains the same as in previous ransom notes.

New Ragnar Locker Victim Post Provides Insight to TTPs; Indications of Collaborations Between BGH Operators

A recent post by VIKING SPIDER on their dedicated leak site (DLS) detailing a new victim has provided insight to the operator's TTPs (CSA-200822). The post alludes to the actors exploiting vulnerabilities to secure initial access and moving laterally through the network after successfully elevating permissions to "Domain admin" level. Although the exact vulnerabilities exploited are unconfirmed, the information provides important insights to VIKING SPIDER's modus operandi.

There is increasing evidence of a collaboration or business relationship between VIKING SPIDER and the big game hunting (BGH) operators TWISTED SPIDER. Earlier in June, the two adversaries hosted victim information from each other's operations on their DLSs (CSA-200745). Both have reiterated their intent to refrain from targeting healthcare entities during the current pandemic, and both draw attention to their victims' security issues. This collaborative activity is unique in the current BGH threat landscape, with Ransomware-as-a-Service (RaaS) and affiliate programs the more commonly observed business arrangement.

Spam Campaign Mimicking Italian Revenue Agency Distributes Gozi ISFB

An Italian-language spam campaign involving emails mimicking the Italian Revenue Agency was observed on 29 June 2020 distributing the *Gozi ISFB* banking trojan (CSA-200842). The emails included Excel 4.0 macro documents, and referenced two articles of Italian legislation regarding tax refunds—the timing of the campaign was highly likely intended to coincide with Italy's annual tax deadline of 30 June. Phishing campaigns involving Excel 4.0 macro documents have become increasingly popular during 2020 (CSA-200461). In contrast to typical macro documents, which contain Visual Basic for Applications (VBA) macros, these documents use Excel 4.0 macros that predate VBA macros. It is likely adversaries are using Excel 4.0 macro documents to evade email and host-based security tools that are likely optimized to detect and prevent embedded VBA macros.

DanaBot Sub-Botnet 4 Distributing Avaddon Ransomware

SCULLY SPIDER's *DanaBot* sub-botnet 4 was observed by CrowdStrike Intelligence distributing *Avaddon* ransomware between 22 and 30 June 2020 (CSA-200846). This is the first instance of the sub-botnet delivering this ransomware variant—previous payloads delivered by sub-botnet 4 include WIZARD SPIDER's *Trickbot*, SMOKY SPIDER's *SmokeBot*, and various information stealers and remote administration tools (RATs).

Avaddon has previously been distributed in spam campaigns, including one campaign in June 2020 involving the *Phorpiex* malware targeting Japanese email addresses (CSA-200752). This Avaddon campaign was seemingly opportunistic, with no explicit sector or geographic focus identified.

INDRIK SPIDER's WastedLocker Continues to Grow Victim Base; BGH Operators Continue to Add Victim Details to DLS

INDRIK SPIDER has continued to target organizations primarily in the UK and North America using their new ransomware variant *WastedLocker* (CSA-200824). CrowdStrike Intelligence sensitive source reporting has confirmed 22 victims to date, with the manufacturing sector the most heavily targeted. Despite the naming of two key members of INDRIK SPIDER in unsealed indictments and others in financial sanctions, the group has continued to show resilience in their campaigns. *BitPaymer* operations have not been observed since mid-March 2020, and distribution of *Dridex* was last observed in late March 2020 (CSA-200403). The development and use of WastedLocker is likely intended to distance INDRIK SPIDER from their previous Dridex and BitPaymer operations—though similarities between BitPaymer and WastedLocker suggest such separation has not been fully achieved.

Alongside the identification of new WastedLocker victims, several other BGH operators added details of their victims to their associated DLS this week (see Figure 1).

Figure 1. BGH Ransomware Victims by Sector and Country (26 June to 2 July 2020)

Commodity Malware Updates and Underground Forum Activity; Stolen Datasets Advertised for Sale

Several updates, new releases, and advertisements were identified by CrowdStrike Intelligence within the past week on various criminal and underground forums for commodity malware variants (see summary in Table 1).

DATE	MALWARE	DETAILS
24 June 2020	Taurus Project Stealer	Update to newly released v1.4 • New panel includes loader statistics • Filter added for file grabber function • Wasabi and Daedalus collection added • Domain Detect redesigned
24 June 2020	Raccoon Stealer	Updates made to two versions: • Minor fixes and improvements to v1.5.12 • Added Chromium-based Microsoft Edge browser support for v1.5.13 • Bug fixed affecting auto-encryption in v1.5.13 • Downtime planned between 1 and 4 July 2020 for back-end update
25 June 2020	Buer Loader	Updates for v1.3.7 • Runtime cleaning • Added a loader directory for Windows Defender exceptions • Updated anti-virus
26 June 2020	Avaddon Ransomware	Updates to the build, including • Minor improvements and bug fixes • Panel access updated Ongoing recruitment for “networkers” Vendor urged customers to update to the latest version

26 June 2020	Triumph Loader	Update to v1.2.1 • Small update to the boot-loader • General improvements to the loader
29 June 2020	Amadey Loader	Update to v1.90 • File upload algorithm redesigned, and number of attempts to contact command-and-control (C2) server increased to 5 • Loader will reattempt at later date if target server is busy
29 June 2020	Oski Stealer	Update to v1.9.1, whereby helper DLLs downloaded from C2 are now obfuscated

Table 1. Commodity Malware Updates and Adverts

Also identified by CrowdStrike Intelligence sensitive sources are advertisements for various stolen datasets. These advertisements provide a snapshot of the type of information available to purchase or acquire from eCrime adversaries that can be used to perform phishing attacks or other fraudulent activity.

- A user on an underground forum known for database dumps and leaks recently shared a link to a dataset sourced from an Indian e-commerce platform. The data included personally identifiable information (PII) and contact details, including telephone numbers and postal addresses.
- On 26 June 2020, an Iranian eCrime actor advertised for sale the business credit card details for a U.S.-based commercial real estate company. The details were priced at $120 USD.
- A user with a proven track record of selling stolen government and academia-related databases advertised in June 2020 the sale of a database allegedly sourced from the Saudi Ministry of Interior. The data includes passport details, user records, and some travel-related information. The dataset is priced at $1,000 USD.

The Operators of Joker's Stash and Brian's Club Release Multiple Offerings of Compromised Payment Card Information with PII

The operators of Joker's Stash card shop released one offering from their three recent major breaches this week, BIGBADABOOM-III-US-part57. CrowdStrike Intelligence expects the weekly release of compromised payment card data from the NEW WORLD ORDER, BIGBADABOOM-III, and NIRVANA (releases advertised as LOTUS) breaches to continue, based on the historical activity of Joker's Stash card shop. Additionally, the operators of Joker's Stash released four offerings of compromised payment card data that contained personally PII from the U.S., EU, and other unspecified regions of the world. The abbreviation VBV in the offering highly likely indicates that it contains additional information to successfully bypass or complete Verified by Visa (VBV) fraud protection.

DATE	RELEASE NAME	REGION	NO. OF CARDS
27 June 2020	BIGELEPHANT-FULLINFO-	U.S./EU/World	10,000

	DOB-VBV		
29 June 2020	PINEAPPLE-FULLINFO-DOB-VBV	U.S./EU/World	15,000
30 June 2020	BEAUTIFULLIFE-FULLINFO-DOB-VBV	U.S./EU/World	15,000
1 July 2020	CULTURALSHOCK-FULLINFO-MIX	U.S./EU/World	1,000
1 July 2020	BIGBADABOOM-III-US-part57	U.S.	

Table 2. Recent Joker's Stash Card Shop Releases for 25 June - 2 July 2020

From 25 June to 2 July 2020, CrowdStrike Intelligence sources observed the card shop Brian's Club post five releases of compromised payment card information containing PII and included the cardholder's date of birth (DOB) and Social Security number (SSN).

DATE	RELEASE NAME	REGION	PII
25 June 2020	0625_US_IP_SSN	U.S.	DOB, SSN
26 June 2020	0626_US_IP_SSN	U.S.	DOB, SSN
27 June 2020	0627_US_IP_SSN	U.S.	DOB, SSN
28 June 2020	0628_US_IP_SSN	U.S.	DOB, SSN
29 June 2020	0629_US_IP_SSN	U.S.	DOB, SSN

Table 3. Brian's Club PII Offerings for 25 June- 2 July 2020

TARGETED INTRUSION

WICKED PANDA Deploys RouterGod Malware in Targeted Attacks Against Southeast Asian Entities

As part of ongoing targeted activity against Southeast Asian entities, CrowdStrike Falcon OverWatch detected the deployment of novel malware, named *RouterGod*, at an entity associated with the aviation industry in Hong Kong. This malware has likely been used to target entities in Hong-Kong, Macau, and Taiwan with the actor also deploying additional tools such as *Cobalt Strike*, *DarkShell*, and *Proxip* as part of the same campaign. The Proxip and Cobalt Strike samples are configured to use subdomains of `livehost[.]live`, a domain used by WICKED PANDA as part of ShadowPad activity targeting Hong Kong-based universities in 2019 (CSA-200151). Because of the re-use of this low prevalence domain, continued targeting of Southeast Asian entities as well as the deployment of Proxip and Cobalt Strike in tandem, CrowdStrike Intelligence currently attributes this activity to WICKED PANDA with high confidence.

The name RouterGod is used internally by the malware developers, likely due to the ability of the malware to route encrypted command packets between infected hosts. RouterGod is a .NET executable that can be used to execute arbitrary scripts as well as establish sessions with other infected hosts. Multiple instances of the malware can be used in a chain to deliver implant tasking to specific endpoints within victim networks. Additional technical analysis is available in CSA-200848.

Novel Malware Families Loosely Linked to China Identified

This week, CrowdStrike Intelligence released initial analytic findings on newly identified malware. Both malware families were used in operations consistent with Chinese state-nexus activity:

- In June 2020, CrowdStrike Falcon OverWatch observed an unknown adversary deploy novel malware as part of an attempted compromise at a Southeast Asian IT services provider. The deployed malware uses a legitimate antivirus product executable to gain execution via dynamic link library (DLL) search-order hijacking in order to execute a malicious loader DLL that, in turn, decrypts and loads an associated payload file. Additional activity observed included the execution of a Cobalt Strike stager executable that was used to download an additional payload as well as PowerShell commands used to contact unknown infrastructure. See CSA-200849 for more information.

- Also in June 2020, CrowdStrike Falcon OverWatch identified two closely related incidents at an East Asian multinational pharmaceutical company. Both instances featured a previously unseen implant linked to activity CrowdStrike has assessed as consistent with Chinese state interests. For this activity, legitimate VirtualBox executables were used to host malicious DLLs that in turn load and deobfuscate the malicious payloads. See CSA-200833 for more information.

IMPERIAL KITTEN Continues Operations Against Probable Saudi Arabian Technology Organizations with New FireBAK Variant

CrowdStrike Intelligence has identified continued activity from the Iranian state-nexus IMPERIAL KITTEN adversary throughout the first half of 2020. The activity consisted of the apparent continued development of its *FireBAK* implant, with new variants written in PowerShell and Visual Basic Script (VBS). Additional deployment of the adversary's custom *LaZagne* variant were identified in late June 2020. Additional data suggests that current IMPERIAL KITTEN operations likely focus on technology-related organizations in Saudi Arabia. For more information, see CSA-200843.

New LampCarrier Cluster Activity and Infrastructure Identified

CrowdStrike Intelligence has discovered previously unidentified activity attributed to the LampCarrier cluster including Golang-based malware, a Microsoft Office document containing a malicious macro, and previously unidentified infrastructure. Previously observed LampCarrier activity did not include malware as a significant part of its toolset, as the actor preferred to rely on living-off-the land techniques. The discovery of new malware and malicious documents indicates LampCarrier is evolving its TTPs, particularly in how it establishes persistence on victim networks. Additional information and Indicators of Compromise (IOCs) are available in CSA-200831.

HACKTIVISM

MENA Hacktivists Engage in Doxxing and Defacement Activity

On 28 June 2020, hacktivist group *Oman Hackers* claimed to have doxxed more than 20 individuals they believe responsible for managing social media accounts conducting information operations against Omani interests. The vast majority of the purportedly doxxed individuals were Emirati,

although some citizens of other countries in the Middle East and North Africa (MENA) were also identified. The Oman Hackers group claim to have obtained this information by compromising a fake account managed by one of the doxxed individuals and then identifying additional accounts involved in coordinating inauthentic behavior. In particular, the Oman Hackers group focused its doxxing efforts on three individuals whom the group believes to have ties to various Emirati government and security institutions as well as some legal and media organizations. The Oman Hackers group is currently highly active, continuing to claim that an organized conspiracy is harming the Omani government, its regime, and the country's relations with neighboring countries. For more information, see CSA-200836.

Throughout June 2020, hacktivists operating under the moniker *Moroccan Revolution* have reported more than 1200 notifications to the website defacement archive Zone-H. While the group has been active since at least 2015, June 2020 marked a significant increase in defacement claims. Only two of the defacements listed in Zone-H records noted defacements of government websites in June, both of which were in Vietnam. The defacement activity is very likely opportunistic in nature rather than specifically targeted, due to the large number of defacements with no clear geographic or sector targeting theme. While CrowdStrike Intelligence has not independently attributed the geographic origins of most members claiming association with the group, Moroccan Revolution likely consists broadly of North African hacktivists or individuals sympathetic to issues in the region. Additional information is available in CSA-200828.

Fallout from BlueLeaks Release of Sensitive U.S. Law Enforcement Data

On 19 June 2020, hacktivist-journalist entity Distributed Denial of Secrets (*DDOS*) released 269 GB of materials belonging to hundreds of law enforcement agencies across the U.S., naming the collection BlueLeaks (CSA-200801). The release coincided with protests against U.S. law enforcement agencies after the killing of George FLOYD on 25 May and follows similar protests against law enforcement in Latin America (LATAM). Journalist and operator of DDOS Emma BEST—known to work closely with sophisticated hacktivist MOLOTOV JACKAL and has an established track record of publishing materials in the advancement of anti-capitalist and other ideologies (CSA-200663)—made an open call for breaches of U.S. police forces, requesting that hacktivists leak any exfiltrated data to DDOS (CSA-200697). BlueLeaks leveraged at least three simultaneous means of access and distribution: a searchable web portal, a Tor mirror for the portal, and a downloadable Torrent file for the full collection; recent leaks of sensitive law enforcement data in LATAM were published in a similar manner, with a user-friendly GUI enabling easier digestion of the data (CSIT-19233).

Among the BlueLeaks data were sensitive documents belonging to the Maine Information and Analysis Center (MIAC). Internal MIAC communication was allegedly not compromised but results of requests for information (RFIs) were exposed, including personally identifiable information (PII) of subjects and victims as well as information regarding ongoing investigations in Maine. It was also revealed that MIAC has been closely tracking Black Lives Matter (BLM) events and advocacy groups (CSDR-20075).

Hacktivist Campaign Protests Colombian Military Scandal

On 26 June 2020, hacktivist group *Anonymous Colombia* posted an English-language video announcing a campaign to protest acts of extreme violence seven Colombian soldiers committed against indigenous children. The group claimed credit for a DDoS attack and website defacement against two separate websites belonging to former Colombian president and current Senator Álvaro URIBE. A separate hacktivist group known as *Anonym0us China* backed the campaign, claiming responsibility for a DDoS attack of the Colombian Army's English and Spanish-language websites. This operation was the second Anonymous-linked #OpColombia campaign announced that week;

there has been no observed overlap between the actors claiming the activities, highlighting the decentralized nature of the Anonymous movement. For more information, see CSA-200839.

Iranian Hacktivists Target Israeli, U.S. Based Entities

Iranian hacktivist group *Death Squads* claimed credit for a DDoS attack against the domains of an Israeli domain registrar and a U.S.-based bank. As the veracity and credibility of these attacks cannot be confirmed, the attack and associated denial of service were likely limited in duration and effect. Death Squads' latest claims represent a departure from past efforts and are assessed to likely be geopolitically motivated due to the group's nationalistic outlook and the backgrounds of its core membership. This effort is likely of low sophistication and representative of a singular hacktivist effort rather than part of a wider campaign. See CSA-200837 for more information.

The timing of the claim also coincides with additional (though apparently unrelated) attacks claimed by Iranian hacktivist groups *Vortex Security Team* and *Unidentified Security Team* against Israel. Specifically, the groups claimed what appear to be two distinct alleged intrusions: one targeting an Israeli gas company's server and the other against an unknown entity. The server is assessed to likely have been identified via exposed services or port-scanning activity; the propensity of hacktivists to conflate publicly available information with data breaches suggests there are even chances the extent of the intrusion was either exaggerated or extremely limited in scale. The hacktivist groups claim that a 27 June explosion near an Iranian military base on 24 June was a result of an Israeli cyberattack, and the groups took retaliatory action in response. For further reading, see CSA-200840.

DATA EXPOSURE & BREACHES

Threat Actor Reportedly Selling Data Stolen From 14 Companies

A threat actor is reportedly selling databases stolen from 14 different companies on an underground forum, according to media reports.[1] Stolen data varies per company, though all breaches reportedly include usernames and hashed passwords. The threat actor is selling the databases at varying prices, ranging from $100 to $1,100 USD. The companies were all allegedly breached in 2020, though the exact dates of compromise, if true, remains unknown. Of the fourteen companies, four companies have previously reported breaches. It is currently unclear if the stolen databases from those four companies are connected to the previously reported breaches.

Eight U.S. Cities Reportedly Impacted by Click2Gov Breaches

The local governments of eight U.S.-based cities discovered a JavaScript (JS) skimmer had been injected into the payment portals of their Click2Gov sites.[2] The eight cities were located across three U.S. states. Industry researchers disclosed two different exfiltration servers that hosted the JS skimmer; one server was used for three sites and one used for the remaining five sites. The JS skimmer was designed to collect payment card information, including card number, expiration date, and CVV, as well as names and physical addresses. Media reports speculate that these compromises are the result of a threat group leveraging *Magecart* tactics. However, CrowdStrike Intelligence does not currently attribute this activity to a known adversary at this time.

Recent Reporting

CSIT-20100 Analysis of TRACER KITTEN DNSDAT Malware Targeting the Middle Eastern Telecommunications Sector

This Tipper provides technical analysis of the *DNSDAT* malware in use by the Iranian actor TRACER KITTEN.

CSMR-20005 CrowdStrike Intelligence Monthly Report - May 2020

This report provides significant analytic findings from May 2020, including trends observed in targeted intrusion, eCrime, and hacktivist operations.

[1] https[:]//www.bleepingcomputer[.]com/news/security/seller-floods-hacker-forum-with-data-stolen-from-14-companies/

[2] https[:]//blog.trendmicro[.]com/trendlabs-security-intelligence/us-local-government-services-targeted-by-new-magecart-credit-card-skimming-attack/

Access to linked reports require Falcon X Premium. Learn more | Manage subscription | Contact us

Copyright © 2020 CrowdStrike, Inc. All rights reserved.

CSWR-20025 CrowdStrike Intelligence Weekly Report: Week of 06/27/2020

To:	Jonathan Springborn (Sheriff), Keith Morrison (Sheriff), Christopher Moore (Sheriff)
Sent:	July 3, 2020 3:33:19 PM CDT
Received:	July 3, 2020 3:33:24 PM CDT

[GovQA] FOIA Request - Activity Assignment ~~:: R009142-062920 - 4766

From: Cook County Sheriff's Office <cookcountysheriff@govqa.us>
To: Christopher.Seaman@cookcountyil.gov, Christopher Seaman (Sheriff) <Christopher.Seaman@cookcountyil.gov>

Sent: July 6, 2020 10:04:05 AM CDT
Received: July 6, 2020 10:04:09 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Attorney-Client Privilege

A task has been assigned to you to Provide Records on Request FOIA Request / #R009142-062920
Activity #4766

CLICK HERE TO COMPLETE THIS ACTIVITY ASSIGNMENT

Activity Information
Activity Assigned Staff: Christopher Seaman
Activity Type: Provide Employee Records
Due Date: 7/13/2020
Activity Summary: Please let me know what is returned in keyword search "BlueLeaks" for 11/1/2018 - present

FOIA Request for Records
Assigned Staff: Elizabeth Scannell
Status: Received
Create Date: June 29, 2020
Due Date: July 06, 2020
Name of Requester: Emma Best
Requester Affiliation: Press
Record(s) Requested: To Whom It May Concern: Pursuant to the Illinois Freedom of Information Act., I hereby request the following records: 1. Documents mentioning, describing or generated in response to the BlueLeaks release, the preceding hack or subsequent fallout, including but not limited to: * Damage assessments * Emails * Interagency communications (local, state, or federal) * Communications with the press about BlueLeaks * Communications with Twitter or other social media or sharing platforms 2. Documents mentioning or describing Distributed Denial of Secrets (DDoSecrets) You may limit this request to records generated between November 1, 2018 and the present. I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers in outlets such as Gizmodo, MuckRock, Motherboard, Property of the People, Unicorn Riot, and The Outline, among others. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In

addition, I discuss and comment on the files online and make them available through non-profits such as the library Internet Archive and the journalist non-profit MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself. As such, it is not necessary for me to demonstrate the relevance of this particular subject in advance. As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived. The requested documents will be made available to the general public, and this request is not being made for commercial purposes. In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not. Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 5 business days, as the statute requires. Sincerely, Emma Best Upload documents directly: https://https://www.muckrock.comhttps://accounts.muckrock.com/accounts/login/?next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fcook-county-sheriff-719%252Fblueleaks-cook-county-sheriff-96941%252F%253F&url_auth_token=AAAaaJnszUVssmdgx6fh2R-tE3U%3A1jppAE%3ADWZbgy7n864OATjAMxtAsPZltYs

This is an auto-generated email and has originated from an unmonitored email account. Please DO NOT REPLY to this email as the contents of your response and any attachments may be externally disseminated inadvertently. Click the link above to respond and upload documents for secure internal review.

[GovQA] FOIA Request - Activity Assignment ~~:: R009142-062920 - 4766

To: Christopher Seaman (Sheriff)
Sent: July 6, 2020 10:04:05 AM CDT
Received: July 6, 2020 10:04:09 AM CDT

RE: FOIA

From:	Elizabeth Scannell (Sheriff) <Elizabeth.Scannell@cookcountyil.gov>
To:	Helen Burke (Sheriff) <Helen.Burke@cookcountyil.gov>, Nicholas Scouffas (Sheriff) <Nicholas.Scouffas@cookcountyil.gov>, Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Eryn Hedderman (Sheriff) <Eryn.Hedderman@cookcountyil.gov>, Matthew Walberg (Sheriff) <Matthew.Walberg@cookcountyil.gov>, Breeann Rials (Sheriff) <breeann.rials@cookcountyil.gov>
Cc:	Joseph Ryan (Sheriff) <Joseph.Ryan2@cookcountyil.gov>, Jacquelyn Hedderman (Sheriff) <Jacquelyn.Hedderman@cookcountyil.gov>, Bradley Curry (Sheriff) <Bradley.Curry@cookcountyil.gov>, Kathleen Carmody (Sheriff) <Kathleen.Carmody@cookcountyil.gov>
Sent:	July 7, 2020 10:57:55 AM CDT
Received:	July 7, 2020 10:57:56 AM CDT
Attachments:	Agenda FOIA Meeting for 7.7.20.pdf

See attached for our call,

Beth Scannell
Assistant General Counsel
Cook County Sheriff's Office
50 W. Washington, Room 704
Chicago, Illinois 60602
Desk: 312.603.3979
Mobile: 312.515.5170

The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential and may be subject to applicable attorney-client and/or work product privileges. If you are not the intended recipient of this message or if this message has been addressed to you in error, please alert the sender immediately by reply e-mail and then delete this message and its attachments. Do not deliver, distribute or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action in reliance upon the information contained in this communication or any attachments. Thank you.

-----Original Appointment-----
From: Helen Burke (Sheriff) <Helen.Burke@cookcountyil.gov>
Sent: Tuesday, March 19, 2019 2:48 PM
To: Helen Burke (Sheriff); Nicholas Scouffas (Sheriff); Elizabeth Scannell (Sheriff); Amar Patel (Sheriff); Eryn Hedderman (Sheriff); Matthew Walberg (Sheriff); Breeann Rials (Sheriff)
Cc: Joseph Ryan (Sheriff); Jacquelyn Hedderman (Sheriff); Bradley Curry (Sheriff); Kathleen Carmody (Sheriff)
Subject: FOIA
When: Tuesday, July 7, 2020 11:30 AM-12:00 PM (UTC-06:00) Central Time (US & Canada).
Where: Dial-in number: 515-604-9587; Access code: 711450

UPDATE: *This call has been moved to Tuesday 7/7 at 11:30*

Dial-in number: 515-604-9587

Access code: 711450

(Beth will host)

RE: FOIA

To:	Helen Burke (Sheriff), Nicholas Scouffas (Sheriff), Amar Patel (Sheriff), Eryn Hedderman (Sheriff), Matthew Walberg (Sheriff), Breeann Rials (Sheriff), Abraham Yasin (Sheriff), Tarry Williams (Sheriff), Leo Schmitz (Sheriff), Adriana Morales (Sheriff), Alfonzo Hunter (Sheriff), Amanda Gallegos (Sheriff), Bradley Curry (Sheriff), Brian White (Sheriff), Carmen Gercone (Sheriff), Carmen Ruffin (Sheriff), Christopher Imhof (Sheriff), David Chiko (Sheriff), Erik Roedel (Sheriff), Gregory Ernst (Sheriff), Heather Bock (Sheriff), Jennifer Black (Sheriff), Jerry Baldwin (Sheriff), John Vega (Sheriff), John Webb (Sheriff), Jonathan Myslinski (Sheriff), Joseph Bellettiere (Sheriff), Kathleen Urbanczyk (Sheriff), Kelley Eldridge (Sheriff), Kevin Connelly (Sheriff), Kevin Ruel (Sheriff), Larry Schurig (Sheriff), Lonnie Hollis (Sheriff), Marlon Parks (Sheriff), Matthew Creen (Sheriff), Michael Brady (Sheriff), Michael Lucente (Sheriff), Michael Miller (Sheriff), Patrick Dwyer (Sheriff), Patrick Moerlien (Sheriff), Richard Brogan (Sheriff), Richard O'Brien (Sheriff), Robert Lunk (Sheriff), Ronald Jenkins (Sheriff), Stephen Bouffard (Sheriff), Theodore Stajura (Sheriff), Jason Hernandez (Sheriff), James Moore (Sheriff), Sheriff Intel, Arunas Buntinas (Sheriff), Keith Morrison (Sheriff), Adnan Memon (Sheriff), Douglas Maclean (Sheriff)
Cc:	Joseph Ryan (Sheriff), Jacquelyn Hedderman (Sheriff), Bradley Curry (Sheriff), Kathleen Carmody (Sheriff), Adnan Memon (Sheriff), Douglas Maclean (Sheriff), Marlon Parks (Sheriff), Brian White (Sheriff), Arunas Buntinas (Sheriff), Tarry Williams (Sheriff), Amar Patel (Sheriff)
Sent:	July 7, 2020 10:57:55 AM CDT
Received:	July 7, 2020 10:57:56 AM CDT

RE: FOIA

To:	Helen Burke (Sheriff), Nicholas Scouffas (Sheriff), Amar Patel (Sheriff), Eryn Hedderman (Sheriff), Matthew Walberg (Sheriff), Breeann Rials (Sheriff)
Cc:	Joseph Ryan (Sheriff), Jacquelyn Hedderman (Sheriff), Bradley Curry (Sheriff), Kathleen Carmody (Sheriff)
Sent:	July 7, 2020 10:57:55 AM CDT
Received:	July 7, 2020 10:58:01 AM CDT

RE: FOIA

From:	Elizabeth Scannell (Sheriff) </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=E3F5ADF1BBDC48C9BD4A9BE8268EA25E-ELIZABETH S>
To:	Helen Burke (Sheriff) <Helen.Burke@cookcountyil.gov>, Nicholas Scouffas (Sheriff) <Nicholas.Scouffas@cookcountyil.gov>, Amar Patel (Sheriff) <Amar.Patel@cookcountyil.gov>, Eryn Hedderman (Sheriff) <Eryn.Hedderman@cookcountyil.gov>, Matthew Walberg (Sheriff) <Matthew.Walberg@cookcountyil.gov>, Breeann Rials (Sheriff) <breeann.rials@cookcountyil.gov>
Cc:	Joseph Ryan (Sheriff) <Joseph.Ryan2@cookcountyil.gov>, Jacquelyn Hedderman (Sheriff) <Jacquelyn.Hedderman@cookcountyil.gov>, Bradley Curry (Sheriff) <Bradley.Curry@cookcountyil.gov>, Kathleen Carmody (Sheriff) <Kathleen.Carmody@cookcountyil.gov>
Sent:	July 7, 2020 10:57:55 AM CDT
Received:	July 7, 2020 10:57:00 AM CDT
Attachments:	Agenda FOIA Meeting for 7.7.20.pdf

See attached for our call,

Beth Scannell
Assistant General Counsel
Cook County Sheriff's Office
50 W. Washington, Room 704
Chicago, Illinois 60602
Desk: 312.603.3979
Mobile: 312.515.5170

The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential and may be subject to applicable attorney-client and/or work product privileges. If you are not the intended recipient of this message or if this message has been addressed to you in error, please alert the sender immediately by reply e-mail and then delete this message and its attachments. Do not deliver, distribute or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action in reliance upon the information contained in this communication or any attachments. Thank you.

-----Original Appointment-----
From: Helen Burke (Sheriff) <Helen.Burke@cookcountyil.gov>
Sent: Tuesday, March 19, 2019 2:48 PM
To: Helen Burke (Sheriff); Nicholas Scouffas (Sheriff); Elizabeth Scannell (Sheriff); Amar Patel (Sheriff); Eryn Hedderman (Sheriff); Matthew Walberg (Sheriff); Breeann Rials (Sheriff)
Cc: Joseph Ryan (Sheriff); Jacquelyn Hedderman (Sheriff); Bradley Curry (Sheriff); Kathleen Carmody (Sheriff)
Subject: FOIA
When: Tuesday, July 7, 2020 11:30 AM-12:00 PM (UTC-06:00) Central Time (US & Canada).
Where: Dial-in number: 515-604-9587; Access code: 711450

UPDATE: *This call has been moved to Tuesday 7/7 at 11:30*

Dial-in number: 515-604-9587

Access code: 711450

(Beth will host)

IT Security News Blast - 7-8-2020

From: Mike Hamilton <Michael.Hamilton@CI.Security>
To: Keith.Morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: July 8, 2020 7:14:13 AM CDT
Received: July 8, 2020 7:14:21 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

IT Security News Blast – 7-8-2020

Cyber Command urges orgs to implement F5 patch for BIG-IP configuration interface flaw

U.S. Cyber Command retweeted last Friday F5's advisory to patch immediately the flaw that could unleash a Remote Code Execution (RCE), possibly leading to the creation or deletion files, disability of services, interception of information, run arbitrary system commands and Java code, completely compromise the system, and pursue further targets, such as the internal network.

https://www.scmagazine.com/home/security-news/cyber-command-urges-orgs-to-implement-f5-patch-for-big-ip-configuration-interface-flaw/

You may be distracted by the pandemic but FYI: US Senate panel OK's backdoors-by-the-backdoor EARN IT Act

The idea is that companies would have to "earn" their legal shield – hence the name of the bill, EARN IT – by following the best practices created by the committee. Following significant pushback on those points, the Judiciary Committee made

changes aimed at gaining the full approval of all its members. In the now-OK'd version of the bill, the commission, called the National Commission on Online Child Sexual Exploitation Prevention, would still create its rules but it would be “voluntary” for online platforms to follow them. Instead, if tech companies did follow the commission’s rules, it “would be a defense in any civil suit,” said committee chair Lindsay Graham (R-SC).

https://www.theregister.com/2020/07/06/revised_earn_it_act/

'If the public knew:' Ripple20 shows medical device software cyber weakness

The stakes are high. Last month, researchers discovered vulnerabilities in a popular TCP/IP library from a third-party software vendor Treck used by Baxter and B. Braun infusion pumps, potentially allowing hackers to take control of the devices remotely and alter medication dosages. Baxter downplayed the threat calling it low-risk or "controlled," as defined by the FDA's cybersecurity guidance, while B. Braun said it is working to patch the vulnerable source code.

https://www.medtechdive.com/news/ripple20-medical-device-cybersecurity-software-bill-of-materials/581031/

IT forensics costs post-cyberattack spike 68% year-over-year

While 63% of the cost of a cyberattack for a non-healthcare policyholder went towards IT forensics, just 41% of this cost was dedicated to IT forensics for healthcare clients. Instead, legal costs took the top spot at 48% of the total cyberattack bill of healthcare clients. [...] “Right now, the industry is experiencing a big surge in cases, and demand for IT forensics services is growing,” he said. Meanwhile, there’s also a limited supply of firms offering these services, leading to a jump in the bill for forensics services post-cyberattack.

https://www.insurancebusinessmag.com/us/news/cyber/it-forensics-costs-postcyberattack-spike-68-yearoveryear-227120.aspx

BEC Busts Take Down Multimillion-Dollar Operations

A second case involves Nigerian national Olalekan Jacob Ponle, also known as "Mr.

Woodbery" and "Mark Kain." A criminal complaint accuses him of orchestrating BEC schemes to defraud US companies, which led to attempted or actual losses amounting to tens of millions of dollars. One Chicago company was tricked into sending wire transfers totaling $15.2 million.

https://www.darkreading.com/attacks-breaches/bec-busts-take-down-multimillion-dollar-operations/d/d-id/1338282

Ransomware attack on insurance MSP Xchanging affects clients

Global IT services and solutions provider DXC Technology announced over the weekend a ransomware attack on systems from its Xchanging subsidiary. Xchanging is known as a managed service provider for businesses in the insurance industry but its list of customers includes companies from other fields: financial services, aerospace and defense, automotive, education, consumer packaged goods, healthcare, manufacturing.

https://www.bleepingcomputer.com/news/security/ransomware-attack-on-insurance-msp-xchanging-affects-clients/

Mexico's Central Bank Thwarts Cyber Attack on Its Website [Subscription]

The central bank's protection protocols kicked in, preventing disruption of its financial market processes and payment systems, according to a statement by the bank known as Banxico. The attempt comes two years after hackers hijacked Mexican financial institutions' connections to the country's domestic payment transfer system, operated by Banxico, and got away with at least $15 million. This latest attack was merely on the website and all central bank information and that of other financial institutions[.]

https://news.bloomberglaw.com/privacy-and-data-security/mexicos-central-bank-thwarts-cyber-attack-on-its-website

Defense cuts, cybersecurity and IoT: Five Senate NDAA amendments to know

1. Studying cyber exploitation

2. Cleaner audits
3. The Internet of Things
4. CISA strength
5. One less step for contractors

https://federalnewsnetwork.com/defense-main/2020/07/defense-cuts-cybersecurity-and-iot-five-senate-ndaa-amendments-to-know/

Russian Cyber Gang 'Cosmic Lynx' Focuses on Email Fraud

With the exception of a few French emails sent to targets in France, most of the group's communications are written in English, and its operators know their vocabulary — some emails contain words like "accretive" and "synergistic," both used in their proper context. In fact, the writing is so good that researchers think it may be possible Cosmic Lynx is hiring people to translate the initial emails so their English is nearly perfect, says Crane Hassold, senior director of threat research at Agari. "When you look at a Cosmic Lynx BEC attack, it is miles beyond what we generally see," he says of the group's sophistication.

https://www.darkreading.com/attacks-breaches/russian-cyber-gang-cosmic-lynx-focuses-on-email-fraud/d/d-id/1338291

FBI chief slams Chinese cyberattacks against U.S. calling it 'one of the largest transfers of wealth in human history'

"To achieve its goals and surpass America, China recognizes it needs to make leaps in cutting edge technology, but the sad fact is that instead of engaging in the hard slog of innovation, China often steals American intellectual property and then uses it to compete against the very American companies it victimizes, in effect, cheating twice," he said, adding that the Chinese government targets "research on everything from military equipment to wind turbines."

https://www.cnbc.com/2020/07/07/fbi-chief-slams-chinese-cyberattacks-against-us-hudson-institute.html

FBI Opens a New China-Related Counterintelligence Investigation Every 10 Hours, Director Says

“China is engaged in a whole-of-state effort to become the world’s only superpower by any means necessary,” Wray said. “The greatest long-term threat to our nation’s information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It’s a threat to our economic security—and by extension, to our national security.”

https://www.nextgov.com/cybersecurity/2020/07/fbi-opens-new-china-related-counterintelligence-investigation-every-10-hours-director-says/166706/

LinkedIn was copying every keystroke of users until iOS 14 exposed it

The snooping tactics of LinkedIn were discovered because of the iOS 14 beta’s Universal clipboard privacy feature that instantly detects when a widget or app accesses data on the clipboard. [...] Apparently, the issue is caused by an equality check between the typed content and the clipboard contents. Berger reiterated in his tweets that LinkedIn never stores or transmits clipboard data, and a fix for this problem will be out soon.

https://www.hackread.com/linkedin-copying-user-keystrokel-ios-14-exposed-it/

Cops Seize Server that Hosted BlueLeaks, DDoSecrets Says

Authorities in Germany have seized a server used by the organization that published a trove of US police internal documents commonly known as BlueLeaks, according to the organization’s founder. [...] DDoSecrets has recently taken WikiLeaks mantle as the most influential leaking organization on the internet, publishing several dumps such as data stolen from the Chilean military, and Neo-Nazi messages exchanged on the chat platform Discord.

https://www.vice.com/en_us/article/qj43xq/cops-seize-blueleaks-ddosecrets-server

E-Verify’s “SSN Lock” is Nothing of the Sort

Lest you think your SSN and DOB is somehow private information, you should know this static data about U.S. residents has been exposed many times over in countless

data breaches, and in any case these digits are available for sale on most Americans via Dark Web sites for roughly the bitcoin equivalent of a fancy caffeinated drink at Starbucks.

https://krebsonsecurity.com/2020/07/e-verifys-ssn-lock-is-nothing-of-the-sort/

The death of remote access VPN

The problem with Remote Access VPN is that they are no longer suitable for a mobile workforce with rampant and unabating cybersecurity threats. To emphasize this problem, a Gartner's June 2019 analysis predicts that by 2023, 60% of enterprises will phase out their Remote Access VPN in favor of Zero-Trust Network Access.

https://www.techradar.com/news/the-death-of-remote-access-vpn

Microsoft Seizes Domains Used in COVID-19-Themed Attacks

The US District Court for the Eastern District of Virginia had earlier granted the company permission to seize the domains after Microsoft had filed a civil complaint about the attacks causing it "irreparable and ongoing harm." Tom Burt, Microsoft corporate vice president, customer security and trust, today likened the attacks to a form of business email compromise that targeted customers in 62 countries.

https://www.darkreading.com/operations/microsoft-seizes-domains-used-in-covid-19-themed-attacks/d/d-id/1338293

Citrix Bugs Allow Unauthenticated Code Injection, Data Theft

Attacks on the management interface of the products could result in system compromise by an unauthenticated user on the management network; or system compromise through cross-site scripting (XSS). Attackers could also create a download link for the device which, if downloaded and then executed by an unauthenticated user on the management network, could result in the compromise of a local computer.

https://threatpost.com/citrix-bugs-allow-unauthenticated-code-injection-data-

theft/157214/

Microsoft Launches Free Linux Forensics and Rootkit Malware Detection Service

Microsoft has announced a new free-to-use initiative aimed at uncovering forensic evidence of sabotage on Linux systems, including rootkits and intrusive malware that may otherwise go undetected. The cloud offering, dubbed Project Freta, is a snapshot-based memory forensic mechanism that aims to provide automated full-system volatile memory inspection of virtual machine (VM) snapshots, with capabilities to spot malicious software, kernel rootkits, and other stealthy malware techniques such as process hiding.

https://thehackernews.com/2020/07/microsoft-linux-forensics-rootkit.html

Exposed dating service databases leak sensitive info on romance-seekers

Independent VPN review site WizCase has reported finding six separate dating sites or apps that each potentially compromised thousands of users due to improper data storage. According to WizCase researchers, the vast majority of the affected accounts belong to Japanese dating sites Charincharin.net and kyuun-kyuun.com, which share the same database. [...] “Every server was easily accessible via the internet and not password protected,” the report stated.

https://www.scmagazine.com/home/security-news/database-security/exposed-dating-service-databases-leak-sensitive-info-on-romance-seekers/

You are receiving this email because you are subscribed to receive the IT Security Daily Blast email from Michael Hamilton, Founder, President, and CISO of CI Security, formerly Critical Informatics.

Archived articles are available at https://ci.security/news/daily-news.

CI Security and the CI Security logo are the trademarks of CI Security, Inc. All other brand names, trademarks, service marks, and copyrights are the property of their respective owners.

© 2020 CI Security. All rights reserved.

245 4th St, Suite 405 Bremerton, WA 98337

Add this Email to Your Address Book

unsubscribe

IT Security News Blast - 7-8-2020

From: Mike Hamilton <Michael.Hamilton@CI.Security>
To: christopher.moore@cookcountyil.gov, Christopher Moore (Sheriff) <Christopher.Moore@cookcountyil.gov>

Sent: July 8, 2020 7:14:13 AM CDT
Received: July 8, 2020 7:14:20 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

IT Security News Blast – 7-8-2020

Cyber Command urges orgs to implement F5 patch for BIG-IP configuration interface flaw

U.S. Cyber Command retweeted last Friday F5's advisory to patch immediately the flaw that could unleash a Remote Code Execution (RCE), possibly leading to the creation or deletion files, disability of services, interception of information, run arbitrary system commands and Java code, completely compromise the system, and pursue further targets, such as the internal network.

https://www.scmagazine.com/home/security-news/cyber-command-urges-orgs-to-implement-f5-patch-for-big-ip-configuration-interface-flaw/

You may be distracted by the pandemic but FYI: US Senate panel OK's backdoors-by-the-backdoor EARN IT Act

The idea is that companies would have to "earn" their legal shield – hence the name of the bill, EARN IT – by following the best practices created by the committee. Following significant pushback on those points, the Judiciary Committee made

changes aimed at gaining the full approval of all its members. In the now-OK'd version of the bill, the commission, called the National Commission on Online Child Sexual Exploitation Prevention, would still create its rules but it would be “voluntary” for online platforms to follow them. Instead, if tech companies did follow the commission’s rules, it “would be a defense in any civil suit,” said committee chair Lindsay Graham (R-SC).

https://www.theregister.com/2020/07/06/revised_earn_it_act/

'If the public knew:' Ripple20 shows medical device software cyber weakness

The stakes are high. Last month, researchers discovered vulnerabilities in a popular TCP/IP library from a third-party software vendor Treck used by Baxter and B. Braun infusion pumps, potentially allowing hackers to take control of the devices remotely and alter medication dosages. Baxter downplayed the threat calling it low-risk or "controlled," as defined by the FDA's cybersecurity guidance, while B. Braun said it is working to patch the vulnerable source code.

https://www.medtechdive.com/news/ripple20-medical-device-cybersecurity-software-bill-of-materials/581031/

IT forensics costs post-cyberattack spike 68% year-over-year

While 63% of the cost of a cyberattack for a non-healthcare policyholder went towards IT forensics, just 41% of this cost was dedicated to IT forensics for healthcare clients. Instead, legal costs took the top spot at 48% of the total cyberattack bill of healthcare clients. [...] “Right now, the industry is experiencing a big surge in cases, and demand for IT forensics services is growing,” he said. Meanwhile, there’s also a limited supply of firms offering these services, leading to a jump in the bill for forensics services post-cyberattack.

https://www.insurancebusinessmag.com/us/news/cyber/it-forensics-costs-postcyberattack-spike-68-yearoveryear-227120.aspx

BEC Busts Take Down Multimillion-Dollar Operations

A second case involves Nigerian national Olalekan Jacob Ponle, also known as "Mr.

Woodbery" and "Mark Kain." A criminal complaint accuses him of orchestrating BEC schemes to defraud US companies, which led to attempted or actual losses amounting to tens of millions of dollars. One Chicago company was tricked into sending wire transfers totaling $15.2 million.

https://www.darkreading.com/attacks-breaches/bec-busts-take-down-multimillion-dollar-operations/d/d-id/1338282

Ransomware attack on insurance MSP Xchanging affects clients

Global IT services and solutions provider DXC Technology announced over the weekend a ransomware attack on systems from its Xchanging subsidiary. Xchanging is known as a managed service provider for businesses in the insurance industry but its list of customers includes companies from other fields: financial services, aerospace and defense, automotive, education, consumer packaged goods, healthcare, manufacturing.

https://www.bleepingcomputer.com/news/security/ransomware-attack-on-insurance-msp-xchanging-affects-clients/

Mexico's Central Bank Thwarts Cyber Attack on Its Website [Subscription]

The central bank's protection protocols kicked in, preventing disruption of its financial market processes and payment systems, according to a statement by the bank known as Banxico. The attempt comes two years after hackers hijacked Mexican financial institutions' connections to the country's domestic payment transfer system, operated by Banxico, and got away with at least $15 million. This latest attack was merely on the website and all central bank information and that of other financial institutions[.]

https://news.bloomberglaw.com/privacy-and-data-security/mexicos-central-bank-thwarts-cyber-attack-on-its-website

Defense cuts, cybersecurity and IoT: Five Senate NDAA amendments to know

1. Studying cyber exploitation

2. Cleaner audits
3. The Internet of Things
4. CISA strength
5. One less step for contractors

https://federalnewsnetwork.com/defense-main/2020/07/defense-cuts-cybersecurity-and-iot-five-senate-ndaa-amendments-to-know/

Russian Cyber Gang 'Cosmic Lynx' Focuses on Email Fraud

With the exception of a few French emails sent to targets in France, most of the group's communications are written in English, and its operators know their vocabulary — some emails contain words like "accretive" and "synergistic," both used in their proper context. In fact, the writing is so good that researchers think it may be possible Cosmic Lynx is hiring people to translate the initial emails so their English is nearly perfect, says Crane Hassold, senior director of threat research at Agari. "When you look at a Cosmic Lynx BEC attack, it is miles beyond what we generally see," he says of the group's sophistication.

https://www.darkreading.com/attacks-breaches/russian-cyber-gang-cosmic-lynx-focuses-on-email-fraud/d/d-id/1338291

FBI chief slams Chinese cyberattacks against U.S. calling it 'one of the largest transfers of wealth in human history'

"To achieve its goals and surpass America, China recognizes it needs to make leaps in cutting edge technology, but the sad fact is that instead of engaging in the hard slog of innovation, China often steals American intellectual property and then uses it to compete against the very American companies it victimizes, in effect, cheating twice," he said, adding that the Chinese government targets "research on everything from military equipment to wind turbines."

https://www.cnbc.com/2020/07/07/fbi-chief-slams-chinese-cyberattacks-against-us-hudson-institute.html

FBI Opens a New China-Related Counterintelligence Investigation Every 10 Hours, Director Says

“China is engaged in a whole-of-state effort to become the world’s only superpower by any means necessary,” Wray said. “The greatest long-term threat to our nation’s information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It’s a threat to our economic security—and by extension, to our national security.”

https://www.nextgov.com/cybersecurity/2020/07/fbi-opens-new-china-related-counterintelligence-investigation-every-10-hours-director-says/166706/

LinkedIn was copying every keystroke of users until iOS 14 exposed it

The snooping tactics of LinkedIn were discovered because of the iOS 14 beta’s Universal clipboard privacy feature that instantly detects when a widget or app accesses data on the clipboard. [...] Apparently, the issue is caused by an equality check between the typed content and the clipboard contents. Berger reiterated in his tweets that LinkedIn never stores or transmits clipboard data, and a fix for this problem will be out soon.

https://www.hackread.com/linkedin-copying-user-keystrokel-ios-14-exposed-it/

Cops Seize Server that Hosted BlueLeaks, DDoSecrets Says

Authorities in Germany have seized a server used by the organization that published a trove of US police internal documents commonly known as BlueLeaks, according to the organization’s founder. [...] DDoSecrets has recently taken WikiLeaks mantle as the most influential leaking organization on the internet, publishing several dumps such as data stolen from the Chilean military, and Neo-Nazi messages exchanged on the chat platform Discord.

https://www.vice.com/en_us/article/qj43xq/cops-seize-blueleaks-ddosecrets-server

E-Verify’s “SSN Lock” is Nothing of the Sort

Lest you think your SSN and DOB is somehow private information, you should know this static data about U.S. residents has been exposed many times over in countless

data breaches, and in any case these digits are available for sale on most Americans via Dark Web sites for roughly the bitcoin equivalent of a fancy caffeinated drink at Starbucks.

https://krebsonsecurity.com/2020/07/e-verifys-ssn-lock-is-nothing-of-the-sort/

The death of remote access VPN

The problem with Remote Access VPN is that they are no longer suitable for a mobile workforce with rampant and unabating cybersecurity threats. To emphasize this problem, a Gartner's June 2019 analysis predicts that by 2023, 60% of enterprises will phase out their Remote Access VPN in favor of Zero-Trust Network Access.

https://www.techradar.com/news/the-death-of-remote-access-vpn

Microsoft Seizes Domains Used in COVID-19-Themed Attacks

The US District Court for the Eastern District of Virginia had earlier granted the company permission to seize the domains after Microsoft had filed a civil complaint about the attacks causing it "irreparable and ongoing harm." Tom Burt, Microsoft corporate vice president, customer security and trust, today likened the attacks to a form of business email compromise that targeted customers in 62 countries.

https://www.darkreading.com/operations/microsoft-seizes-domains-used-in-covid-19-themed-attacks/d/d-id/1338293

Citrix Bugs Allow Unauthenticated Code Injection, Data Theft

Attacks on the management interface of the products could result in system compromise by an unauthenticated user on the management network; or system compromise through cross-site scripting (XSS). Attackers could also create a download link for the device which, if downloaded and then executed by an unauthenticated user on the management network, could result in the compromise of a local computer.

https://threatpost.com/citrix-bugs-allow-unauthenticated-code-injection-data-

theft/157214/

Microsoft Launches Free Linux Forensics and Rootkit Malware Detection Service

Microsoft has announced a new free-to-use initiative aimed at uncovering forensic evidence of sabotage on Linux systems, including rootkits and intrusive malware that may otherwise go undetected. The cloud offering, dubbed Project Freta, is a snapshot-based memory forensic mechanism that aims to provide automated full-system volatile memory inspection of virtual machine (VM) snapshots, with capabilities to spot malicious software, kernel rootkits, and other stealthy malware techniques such as process hiding.

https://thehackernews.com/2020/07/microsoft-linux-forensics-rootkit.html

Exposed dating service databases leak sensitive info on romance-seekers

Independent VPN review site WizCase has reported finding six separate dating sites or apps that each potentially compromised thousands of users due to improper data storage. According to WizCase researchers, the vast majority of the affected accounts belong to Japanese dating sites Charincharin.net and kyuun-kyuun.com, which share the same database. [...] “Every server was easily accessible via the internet and not password protected,” the report stated.

https://www.scmagazine.com/home/security-news/database-security/exposed-dating-service-databases-leak-sensitive-info-on-romance-seekers/

You are receiving this email because you are subscribed to receive the IT Security Daily Blast email from Michael Hamilton, Founder, President, and CISO of CI Security, formerly Critical Informatics.

Archived articles are available at https://ci.security/news/daily-news.

CI Security and the CI Security logo are the trademarks of CI Security, Inc. All other brand names, trademarks, service marks, and copyrights are the property of their respective owners.

© 2020 CI Security. All rights reserved.

245 4th St, Suite 405 Bremerton, WA 98337

Add this Email to Your Address Book

unsubscribe

IACP's The Lead: Some US States Consider Police Licensing.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: brian.white@cookcountyil.gov, Brian White (Sheriff) <Brian.White@cookcountyil.gov>

Sent: July 8, 2020 7:48:45 AM CDT
Received: July 8, 2020 7:48:49 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Brian White

Wednesday, July 8, 2020

POLICING & POLICY

Some US States Consider Police Licensing

Bloomberg Law (7/7, Ebert, Subscription Publication) reports, "Government officials in at least a half-dozen states want to make it easier to end the policing careers of abusive officers by making it hard for them to start fresh in new jurisdictions. 'Now is the time, I believe, to begin treating peace officer certificates more like licenses,' said Ohio Gov. Mike DeWine. 'The only way the state can revoke a peace officer certificate today is if that officer is convicted of a felony,' he said in unveiling a proposal to beef up statewide oversight of law enforcement. 'There is no mechanism in Ohio to revoke a certificate for conduct that might be bad, might be horrible, but is not necessarily criminal.'" Bloomberg Law adds, "Occupational licensing proposals for law enforcement have been pitched in recent weeks in California, Illinois, Massachusetts, New Jersey, Ohio, and Michigan. Three of those states – California, Massachusetts, and New Jersey – along with Rhode Island lack any statewide procedure for decertifying officers."

San Diego, California To Put Police Reform Measure On November Ballot

The San Diego Union-Tribune (7/7, Garrick) reports, "Critics of local law enforcement got a key win Tuesday when the San Diego City Council unanimously agreed to place a long-awaited police reform measure on the November ballot." According to the Union-Tribune, "City voters will get a chance this November to create a new police oversight board that would have the power to launch independent misconduct investigations, subpoena witnesses and hold officers more accountable for their

actions. Community leaders and council members said Tuesday's vote was an important milestone that would allow voters to boost transparency and accountability for local police. But they also stressed that much more needs to be done on police reform." The Union-Tribune adds, "Other recent reform efforts in San Diego include a ban on police officers using carotid restraints, new Police Department de-escalation procedures and creation of an Office on Race and Equity."

US House Democrats Include $597 Million For Police Reform In Spending Bill

The Hill (7/7, Elis) reports, "House Democrats included a slew of police reforms, as well as $596.7 million in funding for reform programs, in a proposed spending bill for the 2021 fiscal year, which begins in October." The Hill adds, "The 2021 Commerce, Justice, Science appropriations bill includes $400 million for initiatives that would boost independent investigations of law enforcement, pattern and practice investigations that look for systemic problems in policing, community-based organizations seeking to improve law enforcement and other initiatives. It would also provide $50 million to train local law enforcement on certain best practices, $77.5 million to grant programs to boost police-community relations, $25 million for federal investigations into misconduct and $4 million for civilian review boards."

US Lawmakers Unveil Bill To Defund Police, Provide Reparations

The New York Post (7/7, Nelson) reports that US Reps. Ayanna Pressley (D-MA) and Rashida Tlaib (D-MI) on Tuesday "announced federal legislation to defund police and set up reparations for people who either are black or were harmed by cops." The two lawmakers announced the measure "on a Zoom call," but it "has not yet been introduced." Said Tlaib, "We can start to envision through this bill a new version for public safety – a new vision for public safety, one that protects and affirms Black lives."

The AP (7/7, Stafford) reports, "Dubbed the BREATHE Act, the legislation is the culmination of a project led by the policy table of the Movement for Black Lives, a coalition of more than 150 organizations."

Minnesota Lawmakers Remain Hopeful About Police Reform Efforts

The Minneapolis Star Tribune (7/8, Berkel, Bierschbach) reports, "Minnesota state lawmakers will get another chance at passing police accountability measures into law next week, with Gov. Tim Walz planning to call a special legislative session for the second time this summer." The Star Tribune adds, "Walz said Tuesday he is optimistic that lawmakers can strike a deal on both a public works spending package and on police reforms in the wake of the May death of George Floyd at the hands of Minneapolis police officers." House Democrats "continue to push for a sweeping package of changes to boost community-led alternatives to policing, ban warrior-style training for officers and raise the threshold for using deadly force from 'apparent' to 'imminent' threats to officers and others."

For U.S. Members:

The 2019–2020 Public Safety Officer Medal of Valor is the United States' highest public safety honor that can be awarded to law enforcement officers, emergency medical personnel, and firefighters. This award honors federal, state, local, and tribal public safety officers who have demonstrated exceptional bravery, risking serious injury or death, in the line of duty. The Bureau of Justice Assistance is seeking nominations for the Medal of Valor now through **Friday, July 31, 2020.**

Public Safety Officers can be nominated for any qualifying event between June 1, 2019, and May 31, 2020. Public Safety Officers must be nominated by the heads of their agencies by July 31, 2020, at 11:59 p.m. ET to be considered for this award. Agency heads may submit multiple nominations to honor several officers or to honor one officer for multiple separate events. Nomination guidelines and stories of past recipients can be found on the Medal of Valor website.

Connect with the IACP online: **IACP Event Calendar:**

CRIME & DRUGS

Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests

USA Today (7/7, Philimon) reports that a "range of disturbing incidents have happened since George Floyd's death and subsequent protests against racism and police brutality." In Illinois, for example, "a man was charged with a hate crime for allegedly riding his motorcycle into a protest and hitting two people," and "authorities say a KKK leader tried to run his car through a group of peaceful protesters in Virginia."

The Washington Examiner (7/7, Smith), meanwhile, reports that "two white residents of Martinez, California, who painted over a Black Lives Matter mural, have been charged with a hate crime."

The Wall Street Journal (7/7, Kusisto, Frosch, Subscription Publication) reports Floyd's death has also prompted the reexamination of older cases by local prosecutors.

New York City Police Arrest 195 In Fireworks Crackdown

WNBC-TV New York (7/7) reports, "Nearly 200 illegal fireworks have been made in New York City in the two weeks since Mayor Bill de Blasio unveiled a multi-agency task force to crack down on the problem amid an unprecedented level of complaints, officials said Tuesday." WNBC-TV adds, "The mayor revealed the task force, comprised of 10 officers with the NYPD Intelligence Bureau, 12 FDNY Fire Marshals and 20 Sheriff's Bureau of Criminal Investigation members, on June 23. Its primary goal: to disrupt illegal fireworks supply chains via sting operations within and outside New York City – and officials say the group busted a total of 195 people since it was established. It's not clear what prompted the extraordinary surge in illegal fireworks usage, which prompted sleep-deprived New Yorkers to protest in front of Gracie Mansion one night last month amid continued booming."

Protesters Charged With Leaking Police Document In Iowa

The AP (7/7, Foley) reports, "Prosecutors in Iowa have filed a rarely used leak charge against Black Lives Matter protesters accused of stealing a confidential police document and displaying it during a television news broadcast." The AP adds, "Two protesters are charged with unauthorized dissemination of intelligence data, a felony that carries up to five years in prison. The Iowa Judicial Branch says it's only the second time that the charge has been filed since 2010. It's intended to punish officers and others who share information that could undermine criminal investigations or violate privacy protections." According to the AP, "The document in question was a Des Moines Police Department bulletin that officers and state troopers had with them while patrolling a July 1 protest at the Iowa Capitol. The bulletin included photos of suspects who were wanted in the destruction of a Des Moines police car during a June 20 protest."

Dutch Police Arrest Six, Uncover Makeshift Torture Chamber

The AP (7/7, Corder) reports, "Dutch police arrested six men after discovering sea containers that had been converted into a makeshift prison and sound-proofed 'torture chamber' complete with a dentist's chair, tools including pliers and scalpels and handcuffs, a high ranking officer announced Tuesday. Authorities said police conducted the raid before the torture chamber could be used and alerted potential victims, who went into hiding." The AP adds, "The grisly discovery was made last month by officers investigating leads generated by data from encrypted phones used by criminals. The communications network was cracked recently by French police. Detectives in Britain and the Netherlands have already arrested hundreds of suspects based on the encrypted messages." According to the AP, "Tuesday's announcement gave a chilling insight into the increasingly violent Dutch criminal underworld, which is involved in the large scale production and trafficking of drugs."

TECHNOLOGY

German Authorities Seize Server Hosting "BlueLeaks" Data Dump

PCMag (7/7, Kan) reports, "German authorities have confiscated a server hosting the "BlueLeaks" data dump, a 269GB trove of internal police documents that leaked last month." According to PCMag, "The Wikileaks-style group Distributed Denial

of Secrets (DDOS) had been using the server to enable the public to download the files, but prosecutors in Germany recently seized it, according to Emma Best, a journalist and co-founder of the group. DDOS says it obtained the files from the 'hacktivist' collective Anonymous, and then made the files searchable on a dedicated website on July 19. However, the site now appears to be down." Best said "German authorities seized the 'primary public download server' hosting the data dump without supplying an explanation. The hosting provider has only said the takedown came from the 'department of public prosecution Zwickau,' which didn't immediately respond to a request for comment."

TUESDAY'S LEAD STORIES

- **Qualified Immunity At Forefront Of Policing Debate**
- **Door Of Portland, Oregon Federal Courthouse Shattered, Fireworks Exploded Inside**
- **New Mexico Militia Was Involved In June Shooting Incident In Albuquerque**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to brian.white@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Some US States Consider Police Licensing.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: keith.morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: July 8, 2020 7:48:45 AM CDT
Received: July 8, 2020 7:48:49 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Keith Morrison

Wednesday, July 8, 2020

POLICING & POLICY

Some US States Consider Police Licensing

Bloomberg Law (7/7, Ebert, Subscription Publication) reports, "Government officials in at least a half-dozen states want to make it easier to end the policing careers of abusive officers by making it hard for them to start fresh in new jurisdictions. 'Now is the time, I believe, to begin treating peace officer certificates more like licenses,' said Ohio Gov. Mike DeWine. 'The only way the state can revoke a peace officer certificate today is if that officer is convicted of a felony,' he said in unveiling a proposal to beef up statewide oversight of law enforcement. 'There is no mechanism in Ohio to revoke a certificate for conduct that might be bad, might be horrible, but is not necessarily criminal.'" Bloomberg Law adds, "Occupational licensing proposals for law enforcement have been pitched in recent weeks in California, Illinois, Massachusetts, New Jersey, Ohio, and Michigan. Three of those states – California, Massachusetts, and New Jersey – along with Rhode Island lack any statewide procedure for decertifying officers."

San Diego, California To Put Police Reform Measure On November Ballot

The San Diego Union-Tribune (7/7, Garrick) reports, "Critics of local law enforcement got a key win Tuesday when the San Diego City Council unanimously agreed to place a long-awaited police reform measure on the November ballot." According to the Union-Tribune, "City voters will get a chance this November to create a new police oversight board that would have the power to launch independent misconduct investigations, subpoena witnesses and hold officers more accountable for their

actions. Community leaders and council members said Tuesday's vote was an important milestone that would allow voters to boost transparency and accountability for local police. But they also stressed that much more needs to be done on police reform." The Union-Tribune adds, "Other recent reform efforts in San Diego include a ban on police officers using carotid restraints, new Police Department de-escalation procedures and creation of an Office on Race and Equity."

US House Democrats Include $597 Million For Police Reform In Spending Bill

The Hill (7/7, Elis) reports, "House Democrats included a slew of police reforms, as well as $596.7 million in funding for reform programs, in a proposed spending bill for the 2021 fiscal year, which begins in October." The Hill adds, "The 2021 Commerce, Justice, Science appropriations bill includes $400 million for initiatives that would boost independent investigations of law enforcement, pattern and practice investigations that look for systemic problems in policing, community-based organizations seeking to improve law enforcement and other initiatives. It would also provide $50 million to train local law enforcement on certain best practices, $77.5 million to grant programs to boost police-community relations, $25 million for federal investigations into misconduct and $4 million for civilian review boards."

US Lawmakers Unveil Bill To Defund Police, Provide Reparations

The New York Post (7/7, Nelson) reports that US Reps. Ayanna Pressley (D-MA) and Rashida Tlaib (D-MI) on Tuesday "announced federal legislation to defund police and set up reparations for people who either are black or were harmed by cops." The two lawmakers announced the measure "on a Zoom call," but it "has not yet been introduced." Said Tlaib, "We can start to envision through this bill a new version for public safety – a new vision for public safety, one that protects and affirms Black lives."

The AP (7/7, Stafford) reports, "Dubbed the BREATHE Act, the legislation is the culmination of a project led by the policy table of the Movement for Black Lives, a coalition of more than 150 organizations."

Minnesota Lawmakers Remain Hopeful About Police Reform Efforts

The Minneapolis Star Tribune (7/8, Berkel, Bierschbach) reports, "Minnesota state lawmakers will get another chance at passing police accountability measures into law next week, with Gov. Tim Walz planning to call a special legislative session for the second time this summer." The Star Tribune adds, "Walz said Tuesday he is optimistic that lawmakers can strike a deal on both a public works spending package and on police reforms in the wake of the May death of George Floyd at the hands of Minneapolis police officers." House Democrats "continue to push for a sweeping package of changes to boost community-led alternatives to policing, ban warrior-style training for officers and raise the threshold for using deadly force from 'apparent' to 'imminent' threats to officers and others."

For U.S. Members:

The 2019–2020 Public Safety Officer Medal of Valor is the United States' highest public safety honor that can be awarded to law enforcement officers, emergency medical personnel, and firefighters. This award honors federal, state, local, and tribal public safety officers who have demonstrated exceptional bravery, risking serious injury or death, in the line of duty. The Bureau of Justice Assistance is seeking nominations for the Medal of Valor now through **Friday, July 31, 2020.**

Public Safety Officers can be nominated for any qualifying event between June 1, 2019, and May 31, 2020. Public Safety Officers must be nominated by the heads of their agencies by July 31, 2020, at 11:59 p.m. ET to be considered for this award. Agency heads may submit multiple nominations to honor several officers or to honor one officer for multiple separate events. Nomination guidelines and stories of past recipients can be found on the Medal of Valor website.

Connect with the IACP online: **IACP Event Calendar:**

CRIME & DRUGS

Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests

USA Today (7/7, Philimon) reports that a "range of disturbing incidents have happened since George Floyd's death and subsequent protests against racism and police brutality." In Illinois, for example, "a man was charged with a hate crime for allegedly riding his motorcycle into a protest and hitting two people," and "authorities say a KKK leader tried to run his car through a group of peaceful protesters in Virginia."

The Washington Examiner (7/7, Smith), meanwhile, reports that "two white residents of Martinez, California, who painted over a Black Lives Matter mural, have been charged with a hate crime."

The Wall Street Journal (7/7, Kusisto, Frosch, Subscription Publication) reports Floyd's death has also prompted the reexamination of older cases by local prosecutors.

New York City Police Arrest 195 In Fireworks Crackdown

WNBC-TV New York (7/7) reports, "Nearly 200 illegal fireworks have been made in New York City in the two weeks since Mayor Bill de Blasio unveiled a multi-agency task force to crack down on the problem amid an unprecedented level of complaints, officials said Tuesday." WNBC-TV adds, "The mayor revealed the task force, comprised of 10 officers with the NYPD Intelligence Bureau, 12 FDNY Fire Marshals and 20 Sheriff's Bureau of Criminal Investigation members, on June 23. Its primary goal: to disrupt illegal fireworks supply chains via sting operations within and outside New York City – and officials say the group busted a total of 195 people since it was established. It's not clear what prompted the extraordinary surge in illegal fireworks usage, which prompted sleep-deprived New Yorkers to protest in front of Gracie Mansion one night last month amid continued booming."

Protesters Charged With Leaking Police Document In Iowa

The AP (7/7, Foley) reports, "Prosecutors in Iowa have filed a rarely used leak charge against Black Lives Matter protesters accused of stealing a confidential police document and displaying it during a television news broadcast." The AP adds, "Two protesters are charged with unauthorized dissemination of intelligence data, a felony that carries up to five years in prison. The Iowa Judicial Branch says it's only the second time that the charge has been filed since 2010. It's intended to punish officers and others who share information that could undermine criminal investigations or violate privacy protections." According to the AP, "The document in question was a Des Moines Police Department bulletin that officers and state troopers had with them while patrolling a July 1 protest at the Iowa Capitol. The bulletin included photos of suspects who were wanted in the destruction of a Des Moines police car during a June 20 protest."

Dutch Police Arrest Six, Uncover Makeshift Torture Chamber

The AP (7/7, Corder) reports, "Dutch police arrested six men after discovering sea containers that had been converted into a makeshift prison and sound-proofed 'torture chamber' complete with a dentist's chair, tools including pliers and scalpels and handcuffs, a high ranking officer announced Tuesday. Authorities said police conducted the raid before the torture chamber could be used and alerted potential victims, who went into hiding." The AP adds, "The grisly discovery was made last month by officers investigating leads generated by data from encrypted phones used by criminals. The communications network was cracked recently by French police. Detectives in Britain and the Netherlands have already arrested hundreds of suspects based on the encrypted messages." According to the AP, "Tuesday's announcement gave a chilling insight into the increasingly violent Dutch criminal underworld, which is involved in the large scale production and trafficking of drugs."

TECHNOLOGY

German Authorities Seize Server Hosting "BlueLeaks" Data Dump

PCMag (7/7, Kan) reports, "German authorities have confiscated a server hosting the "BlueLeaks" data dump, a 269GB trove of internal police documents that leaked last month." According to PCMag, "The Wikileaks-style group Distributed Denial

of Secrets (DDOS) had been using the server to enable the public to download the files, but prosecutors in Germany recently seized it, according to Emma Best, a journalist and co-founder of the group. DDOS says it obtained the files from the 'hacktivist' collective Anonymous, and then made the files searchable on a dedicated website on July 19. However, the site now appears to be down." Best said "German authorities seized the 'primary public download server' hosting the data dump without supplying an explanation. The hosting provider has only said the takedown came from the 'department of public prosecution Zwickau,' which didn't immediately respond to a request for comment."

TUESDAY'S LEAD STORIES

- **Qualified Immunity At Forefront Of Policing Debate**
- **Door Of Portland, Oregon Federal Courthouse Shattered, Fireworks Exploded Inside**
- **New Mexico Militia Was Involved In June Shooting Incident In Albuquerque**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to keith.morrison@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Some US States Consider Police Licensing.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: jennifer.warren@cookcountyil.gov, Jennifer Warren (Sheriff) <jennifer.warren@cookcountyil.gov>

Sent: July 8, 2020 7:48:46 AM CDT
Received: July 8, 2020 7:48:51 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Jennifer Warren

Wednesday, July 8, 2020

POLICING & POLICY

Some US States Consider Police Licensing

Bloomberg Law (7/7, Ebert, Subscription Publication) reports, "Government officials in at least a half-dozen states want to make it easier to end the policing careers of abusive officers by making it hard for them to start fresh in new jurisdictions. 'Now is the time, I believe, to begin treating peace officer certificates more like licenses,' said Ohio Gov. Mike DeWine. 'The only way the state can revoke a peace officer certificate today is if that officer is convicted of a felony,' he said in unveiling a proposal to beef up statewide oversight of law enforcement. 'There is no mechanism in Ohio to revoke a certificate for conduct that might be bad, might be horrible, but is not necessarily criminal.'" Bloomberg Law adds, "Occupational licensing proposals for law enforcement have been pitched in recent weeks in California, Illinois, Massachusetts, New Jersey, Ohio, and Michigan. Three of those states – California, Massachusetts, and New Jersey – along with Rhode Island lack any statewide procedure for decertifying officers."

San Diego, California To Put Police Reform Measure On November Ballot

The San Diego Union-Tribune (7/7, Garrick) reports, "Critics of local law enforcement got a key win Tuesday when the San Diego City Council unanimously agreed to place a long-awaited police reform measure on the November ballot." According to the Union-Tribune, "City voters will get a chance this November to create a new police oversight board that would have the power to launch independent misconduct investigations, subpoena witnesses and hold officers more accountable for their

actions. Community leaders and council members said Tuesday's vote was an important milestone that would allow voters to boost transparency and accountability for local police. But they also stressed that much more needs to be done on police reform." The Union-Tribune adds, "Other recent reform efforts in San Diego include a ban on police officers using carotid restraints, new Police Department de-escalation procedures and creation of an Office on Race and Equity."

US House Democrats Include $597 Million For Police Reform In Spending Bill

The Hill (7/7, Elis) reports, "House Democrats included a slew of police reforms, as well as $596.7 million in funding for reform programs, in a proposed spending bill for the 2021 fiscal year, which begins in October." The Hill adds, "The 2021 Commerce, Justice, Science appropriations bill includes $400 million for initiatives that would boost independent investigations of law enforcement, pattern and practice investigations that look for systemic problems in policing, community-based organizations seeking to improve law enforcement and other initiatives. It would also provide $50 million to train local law enforcement on certain best practices, $77.5 million to grant programs to boost police-community relations, $25 million for federal investigations into misconduct and $4 million for civilian review boards."

US Lawmakers Unveil Bill To Defund Police, Provide Reparations

The New York Post (7/7, Nelson) reports that US Reps. Ayanna Pressley (D-MA) and Rashida Tlaib (D-MI) on Tuesday "announced federal legislation to defund police and set up reparations for people who either are black or were harmed by cops." The two lawmakers announced the measure "on a Zoom call," but it "has not yet been introduced." Said Tlaib, "We can start to envision through this bill a new version for public safety – a new vision for public safety, one that protects and affirms Black lives."

The AP (7/7, Stafford) reports, "Dubbed the BREATHE Act, the legislation is the culmination of a project led by the policy table of the Movement for Black Lives, a coalition of more than 150 organizations."

Minnesota Lawmakers Remain Hopeful About Police Reform Efforts

The Minneapolis Star Tribune (7/8, Berkel, Bierschbach) reports, "Minnesota state lawmakers will get another chance at passing police accountability measures into law next week, with Gov. Tim Walz planning to call a special legislative session for the second time this summer." The Star Tribune adds, "Walz said Tuesday he is optimistic that lawmakers can strike a deal on both a public works spending package and on police reforms in the wake of the May death of George Floyd at the hands of Minneapolis police officers." House Democrats "continue to push for a sweeping package of changes to boost community-led alternatives to policing, ban warrior-style training for officers and raise the threshold for using deadly force from 'apparent' to 'imminent' threats to officers and others."

For U.S. Members:

The 2019–2020 Public Safety Officer Medal of Valor is the United States' highest public safety honor that can be awarded to law enforcement officers, emergency medical personnel, and firefighters. This award honors federal, state, local, and tribal public safety officers who have demonstrated exceptional bravery, risking serious injury or death, in the line of duty. The Bureau of Justice Assistance is seeking nominations for the Medal of Valor now through **Friday, July 31, 2020.**

Public Safety Officers can be nominated for any qualifying event between June 1, 2019, and May 31, 2020. Public Safety Officers must be nominated by the heads of their agencies by July 31, 2020, at 11:59 p.m. ET to be considered for this award. Agency heads may submit multiple nominations to honor several officers or to honor one officer for multiple separate events. Nomination guidelines and stories of past recipients can be found on the Medal of Valor website.

Connect with the IACP online: **IACP Event Calendar:**

CRIME & DRUGS

Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests

USA Today (7/7, Philimon) reports that a "range of disturbing incidents have happened since George Floyd's death and subsequent protests against racism and police brutality." In Illinois, for example, "a man was charged with a hate crime for allegedly riding his motorcycle into a protest and hitting two people," and "authorities say a KKK leader tried to run his car through a group of peaceful protesters in Virginia."

The Washington Examiner (7/7, Smith), meanwhile, reports that "two white residents of Martinez, California, who painted over a Black Lives Matter mural, have been charged with a hate crime."

The Wall Street Journal (7/7, Kusisto, Frosch, Subscription Publication) reports Floyd's death has also prompted the reexamination of older cases by local prosecutors.

New York City Police Arrest 195 In Fireworks Crackdown

WNBC-TV New York (7/7) reports, "Nearly 200 illegal fireworks have been made in New York City in the two weeks since Mayor Bill de Blasio unveiled a multi-agency task force to crack down on the problem amid an unprecedented level of complaints, officials said Tuesday." WNBC-TV adds, "The mayor revealed the task force, comprised of 10 officers with the NYPD Intelligence Bureau, 12 FDNY Fire Marshals and 20 Sheriff's Bureau of Criminal Investigation members, on June 23. Its primary goal: to disrupt illegal fireworks supply chains via sting operations within and outside New York City – and officials say the group busted a total of 195 people since it was established. It's not clear what prompted the extraordinary surge in illegal fireworks usage, which prompted sleep-deprived New Yorkers to protest in front of Gracie Mansion one night last month amid continued booming."

Protesters Charged With Leaking Police Document In Iowa

The AP (7/7, Foley) reports, "Prosecutors in Iowa have filed a rarely used leak charge against Black Lives Matter protesters accused of stealing a confidential police document and displaying it during a television news broadcast." The AP adds, "Two protesters are charged with unauthorized dissemination of intelligence data, a felony that carries up to five years in prison. The Iowa Judicial Branch says it's only the second time that the charge has been filed since 2010. It's intended to punish officers and others who share information that could undermine criminal investigations or violate privacy protections." According to the AP, "The document in question was a Des Moines Police Department bulletin that officers and state troopers had with them while patrolling a July 1 protest at the Iowa Capitol. The bulletin included photos of suspects who were wanted in the destruction of a Des Moines police car during a June 20 protest."

Dutch Police Arrest Six, Uncover Makeshift Torture Chamber

The AP (7/7, Corder) reports, "Dutch police arrested six men after discovering sea containers that had been converted into a makeshift prison and sound-proofed 'torture chamber' complete with a dentist's chair, tools including pliers and scalpels and handcuffs, a high ranking officer announced Tuesday. Authorities said police conducted the raid before the torture chamber could be used and alerted potential victims, who went into hiding." The AP adds, "The grisly discovery was made last month by officers investigating leads generated by data from encrypted phones used by criminals. The communications network was cracked recently by French police. Detectives in Britain and the Netherlands have already arrested hundreds of suspects based on the encrypted messages." According to the AP, "Tuesday's announcement gave a chilling insight into the increasingly violent Dutch criminal underworld, which is involved in the large scale production and trafficking of drugs."

TECHNOLOGY

German Authorities Seize Server Hosting "BlueLeaks" Data Dump

PCMag (7/7, Kan) reports, "German authorities have confiscated a server hosting the "BlueLeaks" data dump, a 269GB trove of internal police documents that leaked last month." According to PCMag, "The Wikileaks-style group Distributed Denial

of Secrets (DDOS) had been using the server to enable the public to download the files, but prosecutors in Germany recently seized it, according to Emma Best, a journalist and co-founder of the group. DDOS says it obtained the files from the 'hacktivist' collective Anonymous, and then made the files searchable on a dedicated website on July 19. However, the site now appears to be down." Best said "German authorities seized the 'primary public download server' hosting the data dump without supplying an explanation. The hosting provider has only said the takedown came from the 'department of public prosecution Zwickau,' which didn't immediately respond to a request for comment."

TUESDAY'S LEAD STORIES

- **Qualified Immunity At Forefront Of Policing Debate**
- **Door Of Portland, Oregon Federal Courthouse Shattered, Fireworks Exploded Inside**
- **New Mexico Militia Was Involved In June Shooting Incident In Albuquerque**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to jennifer.warren@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Some US States Consider Police Licensing.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: noureen.kapadia@cookcountyil.gov, Noureen Kapadia (Sheriff) <Noureen.Kapadia@cookcountyil.gov>

Sent: July 8, 2020 7:48:46 AM CDT
Received: July 8, 2020 7:48:53 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Noureen Kapadia

Wednesday, July 8, 2020

POLICING & POLICY

Some US States Consider Police Licensing

Bloomberg Law (7/7, Ebert, Subscription Publication) reports, "Government officials in at least a half-dozen states want to make it easier to end the policing careers of abusive officers by making it hard for them to start fresh in new jurisdictions. 'Now is the time, I believe, to begin treating peace officer certificates more like licenses,' said Ohio Gov. Mike DeWine. 'The only way the state can revoke a peace officer certificate today is if that officer is convicted of a felony,' he said in unveiling a proposal to beef up statewide oversight of law enforcement. 'There is no mechanism in Ohio to revoke a certificate for conduct that might be bad, might be horrible, but is not necessarily criminal.'" Bloomberg Law adds, "Occupational licensing proposals for law enforcement have been pitched in recent weeks in California, Illinois, Massachusetts, New Jersey, Ohio, and Michigan. Three of those states – California, Massachusetts, and New Jersey – along with Rhode Island lack any statewide procedure for decertifying officers."

San Diego, California To Put Police Reform Measure On November Ballot

The San Diego Union-Tribune (7/7, Garrick) reports, "Critics of local law enforcement got a key win Tuesday when the San Diego City Council unanimously agreed to place a long-awaited police reform measure on the November ballot." According to the Union-Tribune, "City voters will get a chance this November to create a new police oversight board that would have the power to launch independent misconduct investigations, subpoena witnesses and hold officers more accountable for their

actions. Community leaders and council members said Tuesday's vote was an important milestone that would allow voters to boost transparency and accountability for local police. But they also stressed that much more needs to be done on police reform." The Union-Tribune adds, "Other recent reform efforts in San Diego include a ban on police officers using carotid restraints, new Police Department de-escalation procedures and creation of an Office on Race and Equity."

US House Democrats Include $597 Million For Police Reform In Spending Bill

The Hill (7/7, Elis) reports, "House Democrats included a slew of police reforms, as well as $596.7 million in funding for reform programs, in a proposed spending bill for the 2021 fiscal year, which begins in October." The Hill adds, "The 2021 Commerce, Justice, Science appropriations bill includes $400 million for initiatives that would boost independent investigations of law enforcement, pattern and practice investigations that look for systemic problems in policing, community-based organizations seeking to improve law enforcement and other initiatives. It would also provide $50 million to train local law enforcement on certain best practices, $77.5 million to grant programs to boost police-community relations, $25 million for federal investigations into misconduct and $4 million for civilian review boards."

US Lawmakers Unveil Bill To Defund Police, Provide Reparations

The New York Post (7/7, Nelson) reports that US Reps. Ayanna Pressley (D-MA) and Rashida Tlaib (D-MI) on Tuesday "announced federal legislation to defund police and set up reparations for people who either are black or were harmed by cops." The two lawmakers announced the measure "on a Zoom call," but it "has not yet been introduced." Said Tlaib, "We can start to envision through this bill a new version for public safety – a new vision for public safety, one that protects and affirms Black lives."

The AP (7/7, Stafford) reports, "Dubbed the BREATHE Act, the legislation is the culmination of a project led by the policy table of the Movement for Black Lives, a coalition of more than 150 organizations."

Minnesota Lawmakers Remain Hopeful About Police Reform Efforts

The Minneapolis Star Tribune (7/8, Berkel, Bierschbach) reports, "Minnesota state lawmakers will get another chance at passing police accountability measures into law next week, with Gov. Tim Walz planning to call a special legislative session for the second time this summer." The Star Tribune adds, "Walz said Tuesday he is optimistic that lawmakers can strike a deal on both a public works spending package and on police reforms in the wake of the May death of George Floyd at the hands of Minneapolis police officers." House Democrats "continue to push for a sweeping package of changes to boost community-led alternatives to policing, ban warrior-style training for officers and raise the threshold for using deadly force from 'apparent' to 'imminent' threats to officers and others."

For U.S. Members:

The 2019–2020 Public Safety Officer Medal of Valor is the United States' highest public safety honor that can be awarded to law enforcement officers, emergency medical personnel, and firefighters. This award honors federal, state, local, and tribal public safety officers who have demonstrated exceptional bravery, risking serious injury or death, in the line of duty. The Bureau of Justice Assistance is seeking nominations for the Medal of Valor now through **Friday, July 31, 2020.**

Public Safety Officers can be nominated for any qualifying event between June 1, 2019, and May 31, 2020. Public Safety Officers must be nominated by the heads of their agencies by July 31, 2020, at 11:59 p.m. ET to be considered for this award. Agency heads may submit multiple nominations to honor several officers or to honor one officer for multiple separate events. Nomination guidelines and stories of past recipients can be found on the Medal of Valor website.

Connect with the IACP online: **IACP Event Calendar:**

CRIME & DRUGS

Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests

USA Today (7/7, Philimon) reports that a "range of disturbing incidents have happened since George Floyd's death and subsequent protests against racism and police brutality." In Illinois, for example, "a man was charged with a hate crime for allegedly riding his motorcycle into a protest and hitting two people," and "authorities say a KKK leader tried to run his car through a group of peaceful protesters in Virginia."

The Washington Examiner (7/7, Smith), meanwhile, reports that "two white residents of Martinez, California, who painted over a Black Lives Matter mural, have been charged with a hate crime."

The Wall Street Journal (7/7, Kusisto, Frosch, Subscription Publication) reports Floyd's death has also prompted the reexamination of older cases by local prosecutors.

New York City Police Arrest 195 In Fireworks Crackdown

WNBC-TV New York (7/7) reports, "Nearly 200 illegal fireworks have been made in New York City in the two weeks since Mayor Bill de Blasio unveiled a multi-agency task force to crack down on the problem amid an unprecedented level of complaints, officials said Tuesday." WNBC-TV adds, "The mayor revealed the task force, comprised of 10 officers with the NYPD Intelligence Bureau, 12 FDNY Fire Marshals and 20 Sheriff's Bureau of Criminal Investigation members, on June 23. Its primary goal: to disrupt illegal fireworks supply chains via sting operations within and outside New York City – and officials say the group busted a total of 195 people since it was established. It's not clear what prompted the extraordinary surge in illegal fireworks usage, which prompted sleep-deprived New Yorkers to protest in front of Gracie Mansion one night last month amid continued booming."

Protesters Charged With Leaking Police Document In Iowa

The AP (7/7, Foley) reports, "Prosecutors in Iowa have filed a rarely used leak charge against Black Lives Matter protesters accused of stealing a confidential police document and displaying it during a television news broadcast." The AP adds, "Two protesters are charged with unauthorized dissemination of intelligence data, a felony that carries up to five years in prison. The Iowa Judicial Branch says it's only the second time that the charge has been filed since 2010. It's intended to punish officers and others who share information that could undermine criminal investigations or violate privacy protections." According to the AP, "The document in question was a Des Moines Police Department bulletin that officers and state troopers had with them while patrolling a July 1 protest at the Iowa Capitol. The bulletin included photos of suspects who were wanted in the destruction of a Des Moines police car during a June 20 protest."

Dutch Police Arrest Six, Uncover Makeshift Torture Chamber

The AP (7/7, Corder) reports, "Dutch police arrested six men after discovering sea containers that had been converted into a makeshift prison and sound-proofed 'torture chamber' complete with a dentist's chair, tools including pliers and scalpels and handcuffs, a high ranking officer announced Tuesday. Authorities said police conducted the raid before the torture chamber could be used and alerted potential victims, who went into hiding." The AP adds, "The grisly discovery was made last month by officers investigating leads generated by data from encrypted phones used by criminals. The communications network was cracked recently by French police. Detectives in Britain and the Netherlands have already arrested hundreds of suspects based on the encrypted messages." According to the AP, "Tuesday's announcement gave a chilling insight into the increasingly violent Dutch criminal underworld, which is involved in the large scale production and trafficking of drugs."

TECHNOLOGY

German Authorities Seize Server Hosting "BlueLeaks" Data Dump

PCMag (7/7, Kan) reports, "German authorities have confiscated a server hosting the "BlueLeaks" data dump, a 269GB trove of internal police documents that leaked last month." According to PCMag, "The Wikileaks-style group Distributed Denial

of Secrets (DDOS) had been using the server to enable the public to download the files, but prosecutors in Germany recently seized it, according to Emma Best, a journalist and co-founder of the group. DDOS says it obtained the files from the 'hacktivist' collective Anonymous, and then made the files searchable on a dedicated website on July 19. However, the site now appears to be down." Best said "German authorities seized the 'primary public download server' hosting the data dump without supplying an explanation. The hosting provider has only said the takedown came from the 'department of public prosecution Zwickau,' which didn't immediately respond to a request for comment."

TUESDAY'S LEAD STORIES

- **Qualified Immunity At Forefront Of Policing Debate**
- **Door Of Portland, Oregon Federal Courthouse Shattered, Fireworks Exploded Inside**
- **New Mexico Militia Was Involved In June Shooting Incident In Albuquerque**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to noureen.kapadia@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Some US States Consider Police Licensing.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: thomas.conley@cookcountyil.gov, Thomas Conley (Sheriff) <Thomas.Conley@cookcountyil.gov>

Sent: July 8, 2020 7:48:46 AM CDT
Received: July 8, 2020 7:48:52 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Thomas Conley

Wednesday, July 8, 2020

POLICING & POLICY

Some US States Consider Police Licensing

Bloomberg Law (7/7, Ebert, Subscription Publication) reports, "Government officials in at least a half-dozen states want to make it easier to end the policing careers of abusive officers by making it hard for them to start fresh in new jurisdictions. 'Now is the time, I believe, to begin treating peace officer certificates more like licenses,' said Ohio Gov. Mike DeWine. 'The only way the state can revoke a peace officer certificate today is if that officer is convicted of a felony,' he said in unveiling a proposal to beef up statewide oversight of law enforcement. 'There is no mechanism in Ohio to revoke a certificate for conduct that might be bad, might be horrible, but is not necessarily criminal.'" Bloomberg Law adds, "Occupational licensing proposals for law enforcement have been pitched in recent weeks in California, Illinois, Massachusetts, New Jersey, Ohio, and Michigan. Three of those states – California, Massachusetts, and New Jersey – along with Rhode Island lack any statewide procedure for decertifying officers."

San Diego, California To Put Police Reform Measure On November Ballot

The San Diego Union-Tribune (7/7, Garrick) reports, "Critics of local law enforcement got a key win Tuesday when the San Diego City Council unanimously agreed to place a long-awaited police reform measure on the November ballot." According to the Union-Tribune, "City voters will get a chance this November to create a new police oversight board that would have the power to launch independent misconduct investigations, subpoena witnesses and hold officers more accountable for their

actions. Community leaders and council members said Tuesday's vote was an important milestone that would allow voters to boost transparency and accountability for local police. But they also stressed that much more needs to be done on police reform." The Union-Tribune adds, "Other recent reform efforts in San Diego include a ban on police officers using carotid restraints, new Police Department de-escalation procedures and creation of an Office on Race and Equity."

US House Democrats Include $597 Million For Police Reform In Spending Bill

The Hill (7/7, Elis) reports, "House Democrats included a slew of police reforms, as well as $596.7 million in funding for reform programs, in a proposed spending bill for the 2021 fiscal year, which begins in October." The Hill adds, "The 2021 Commerce, Justice, Science appropriations bill includes $400 million for initiatives that would boost independent investigations of law enforcement, pattern and practice investigations that look for systemic problems in policing, community-based organizations seeking to improve law enforcement and other initiatives. It would also provide $50 million to train local law enforcement on certain best practices, $77.5 million to grant programs to boost police-community relations, $25 million for federal investigations into misconduct and $4 million for civilian review boards."

US Lawmakers Unveil Bill To Defund Police, Provide Reparations

The New York Post (7/7, Nelson) reports that US Reps. Ayanna Pressley (D-MA) and Rashida Tlaib (D-MI) on Tuesday "announced federal legislation to defund police and set up reparations for people who either are black or were harmed by cops." The two lawmakers announced the measure "on a Zoom call," but it "has not yet been introduced." Said Tlaib, "We can start to envision through this bill a new version for public safety – a new vision for public safety, one that protects and affirms Black lives."

The AP (7/7, Stafford) reports, "Dubbed the BREATHE Act, the legislation is the culmination of a project led by the policy table of the Movement for Black Lives, a coalition of more than 150 organizations."

Minnesota Lawmakers Remain Hopeful About Police Reform Efforts

The Minneapolis Star Tribune (7/8, Berkel, Bierschbach) reports, "Minnesota state lawmakers will get another chance at passing police accountability measures into law next week, with Gov. Tim Walz planning to call a special legislative session for the second time this summer." The Star Tribune adds, "Walz said Tuesday he is optimistic that lawmakers can strike a deal on both a public works spending package and on police reforms in the wake of the May death of George Floyd at the hands of Minneapolis police officers." House Democrats "continue to push for a sweeping package of changes to boost community-led alternatives to policing, ban warrior-style training for officers and raise the threshold for using deadly force from 'apparent' to 'imminent' threats to officers and others."

For U.S. Members:

The 2019–2020 Public Safety Officer Medal of Valor is the United States' highest public safety honor that can be awarded to law enforcement officers, emergency medical personnel, and firefighters. This award honors federal, state, local, and tribal public safety officers who have demonstrated exceptional bravery, risking serious injury or death, in the line of duty. The Bureau of Justice Assistance is seeking nominations for the Medal of Valor now through **Friday, July 31, 2020.**

Public Safety Officers can be nominated for any qualifying event between June 1, 2019, and May 31, 2020. Public Safety Officers must be nominated by the heads of their agencies by July 31, 2020, at 11:59 p.m. ET to be considered for this award. Agency heads may submit multiple nominations to honor several officers or to honor one officer for multiple separate events. Nomination guidelines and stories of past recipients can be found on the Medal of Valor website.

Connect with the IACP online: **IACP Event Calendar:**

CRIME & DRUGS

Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests

USA Today (7/7, Philimon) reports that a "range of disturbing incidents have happened since George Floyd's death and subsequent protests against racism and police brutality." In Illinois, for example, "a man was charged with a hate crime for allegedly riding his motorcycle into a protest and hitting two people," and "authorities say a KKK leader tried to run his car through a group of peaceful protesters in Virginia."

The Washington Examiner (7/7, Smith), meanwhile, reports that "two white residents of Martinez, California, who painted over a Black Lives Matter mural, have been charged with a hate crime."

The Wall Street Journal (7/7, Kusisto, Frosch, Subscription Publication) reports Floyd's death has also prompted the reexamination of older cases by local prosecutors.

New York City Police Arrest 195 In Fireworks Crackdown

WNBC-TV New York (7/7) reports, "Nearly 200 illegal fireworks have been made in New York City in the two weeks since Mayor Bill de Blasio unveiled a multi-agency task force to crack down on the problem amid an unprecedented level of complaints, officials said Tuesday." WNBC-TV adds, "The mayor revealed the task force, comprised of 10 officers with the NYPD Intelligence Bureau, 12 FDNY Fire Marshals and 20 Sheriff's Bureau of Criminal Investigation members, on June 23. Its primary goal: to disrupt illegal fireworks supply chains via sting operations within and outside New York City – and officials say the group busted a total of 195 people since it was established. It's not clear what prompted the extraordinary surge in illegal fireworks usage, which prompted sleep-deprived New Yorkers to protest in front of Gracie Mansion one night last month amid continued booming."

Protesters Charged With Leaking Police Document In Iowa

The AP (7/7, Foley) reports, "Prosecutors in Iowa have filed a rarely used leak charge against Black Lives Matter protesters accused of stealing a confidential police document and displaying it during a television news broadcast." The AP adds, "Two protesters are charged with unauthorized dissemination of intelligence data, a felony that carries up to five years in prison. The Iowa Judicial Branch says it's only the second time that the charge has been filed since 2010. It's intended to punish officers and others who share information that could undermine criminal investigations or violate privacy protections." According to the AP, "The document in question was a Des Moines Police Department bulletin that officers and state troopers had with them while patrolling a July 1 protest at the Iowa Capitol. The bulletin included photos of suspects who were wanted in the destruction of a Des Moines police car during a June 20 protest."

Dutch Police Arrest Six, Uncover Makeshift Torture Chamber

The AP (7/7, Corder) reports, "Dutch police arrested six men after discovering sea containers that had been converted into a makeshift prison and sound-proofed 'torture chamber' complete with a dentist's chair, tools including pliers and scalpels and handcuffs, a high ranking officer announced Tuesday. Authorities said police conducted the raid before the torture chamber could be used and alerted potential victims, who went into hiding." The AP adds, "The grisly discovery was made last month by officers investigating leads generated by data from encrypted phones used by criminals. The communications network was cracked recently by French police. Detectives in Britain and the Netherlands have already arrested hundreds of suspects based on the encrypted messages." According to the AP, "Tuesday's announcement gave a chilling insight into the increasingly violent Dutch criminal underworld, which is involved in the large scale production and trafficking of drugs."

TECHNOLOGY

German Authorities Seize Server Hosting "BlueLeaks" Data Dump

PCMag (7/7, Kan) reports, "German authorities have confiscated a server hosting the "BlueLeaks" data dump, a 269GB trove of internal police documents that leaked last month." According to PCMag, "The Wikileaks-style group Distributed Denial

of Secrets (DDOS) had been using the server to enable the public to download the files, but prosecutors in Germany recently seized it, according to Emma Best, a journalist and co-founder of the group. DDOS says it obtained the files from the 'hacktivist' collective Anonymous, and then made the files searchable on a dedicated website on July 19. However, the site now appears to be down." Best said "German authorities seized the 'primary public download server' hosting the data dump without supplying an explanation. The hosting provider has only said the takedown came from the 'department of public prosecution Zwickau,' which didn't immediately respond to a request for comment."

TUESDAY'S LEAD STORIES

- **Qualified Immunity At Forefront Of Policing Debate**
- **Door Of Portland, Oregon Federal Courthouse Shattered, Fireworks Exploded Inside**
- **New Mexico Militia Was Involved In June Shooting Incident In Albuquerque**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to thomas.conley@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Some US States Consider Police Licensing.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: theresa.olson@cookcountyil.gov, Theresa Olson (Sheriff) <Theresa.Olson@cookcountyil.gov>

Sent: July 8, 2020 7:48:46 AM CDT
Received: July 8, 2020 7:48:52 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Theresa Olson

Wednesday, July 8, 2020

POLICING & POLICY

Some US States Consider Police Licensing

Bloomberg Law (7/7, Ebert, Subscription Publication) reports, "Government officials in at least a half-dozen states want to make it easier to end the policing careers of abusive officers by making it hard for them to start fresh in new jurisdictions. 'Now is the time, I believe, to begin treating peace officer certificates more like licenses,' said Ohio Gov. Mike DeWine. 'The only way the state can revoke a peace officer certificate today is if that officer is convicted of a felony,' he said in unveiling a proposal to beef up statewide oversight of law enforcement. 'There is no mechanism in Ohio to revoke a certificate for conduct that might be bad, might be horrible, but is not necessarily criminal.'" Bloomberg Law adds, "Occupational licensing proposals for law enforcement have been pitched in recent weeks in California, Illinois, Massachusetts, New Jersey, Ohio, and Michigan. Three of those states – California, Massachusetts, and New Jersey – along with Rhode Island lack any statewide procedure for decertifying officers."

San Diego, California To Put Police Reform Measure On November Ballot

The San Diego Union-Tribune (7/7, Garrick) reports, "Critics of local law enforcement got a key win Tuesday when the San Diego City Council unanimously agreed to place a long-awaited police reform measure on the November ballot." According to the Union-Tribune, "City voters will get a chance this November to create a new police oversight board that would have the power to launch independent misconduct investigations, subpoena witnesses and hold officers more accountable for their

actions. Community leaders and council members said Tuesday's vote was an important milestone that would allow voters to boost transparency and accountability for local police. But they also stressed that much more needs to be done on police reform." The Union-Tribune adds, "Other recent reform efforts in San Diego include a ban on police officers using carotid restraints, new Police Department de-escalation procedures and creation of an Office on Race and Equity."

US House Democrats Include $597 Million For Police Reform In Spending Bill

The Hill (7/7, Elis) reports, "House Democrats included a slew of police reforms, as well as $596.7 million in funding for reform programs, in a proposed spending bill for the 2021 fiscal year, which begins in October." The Hill adds, "The 2021 Commerce, Justice, Science appropriations bill includes $400 million for initiatives that would boost independent investigations of law enforcement, pattern and practice investigations that look for systemic problems in policing, community-based organizations seeking to improve law enforcement and other initiatives. It would also provide $50 million to train local law enforcement on certain best practices, $77.5 million to grant programs to boost police-community relations, $25 million for federal investigations into misconduct and $4 million for civilian review boards."

US Lawmakers Unveil Bill To Defund Police, Provide Reparations

The New York Post (7/7, Nelson) reports that US Reps. Ayanna Pressley (D-MA) and Rashida Tlaib (D-MI) on Tuesday "announced federal legislation to defund police and set up reparations for people who either are black or were harmed by cops." The two lawmakers announced the measure "on a Zoom call," but it "has not yet been introduced." Said Tlaib, "We can start to envision through this bill a new version for public safety – a new vision for public safety, one that protects and affirms Black lives."

The AP (7/7, Stafford) reports, "Dubbed the BREATHE Act, the legislation is the culmination of a project led by the policy table of the Movement for Black Lives, a coalition of more than 150 organizations."

Minnesota Lawmakers Remain Hopeful About Police Reform Efforts

The Minneapolis Star Tribune (7/8, Berkel, Bierschbach) reports, "Minnesota state lawmakers will get another chance at passing police accountability measures into law next week, with Gov. Tim Walz planning to call a special legislative session for the second time this summer." The Star Tribune adds, "Walz said Tuesday he is optimistic that lawmakers can strike a deal on both a public works spending package and on police reforms in the wake of the May death of George Floyd at the hands of Minneapolis police officers." House Democrats "continue to push for a sweeping package of changes to boost community-led alternatives to policing, ban warrior-style training for officers and raise the threshold for using deadly force from 'apparent' to 'imminent' threats to officers and others."

For U.S. Members:

The 2019–2020 Public Safety Officer Medal of Valor is the United States' highest public safety honor that can be awarded to law enforcement officers, emergency medical personnel, and firefighters. This award honors federal, state, local, and tribal public safety officers who have demonstrated exceptional bravery, risking serious injury or death, in the line of duty. The Bureau of Justice Assistance is seeking nominations for the Medal of Valor now through **Friday, July 31, 2020.**

Public Safety Officers can be nominated for any qualifying event between June 1, 2019, and May 31, 2020. Public Safety Officers must be nominated by the heads of their agencies by July 31, 2020, at 11:59 p.m. ET to be considered for this award. Agency heads may submit multiple nominations to honor several officers or to honor one officer for multiple separate events. Nomination guidelines and stories of past recipients can be found on the Medal of Valor website.

Connect with the IACP online: **IACP Event Calendar:**

CRIME & DRUGS

Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests

USA Today (7/7, Philimon) reports that a "range of disturbing incidents have happened since George Floyd's death and subsequent protests against racism and police brutality." In Illinois, for example, "a man was charged with a hate crime for allegedly riding his motorcycle into a protest and hitting two people," and "authorities say a KKK leader tried to run his car through a group of peaceful protesters in Virginia."

The Washington Examiner (7/7, Smith), meanwhile, reports that "two white residents of Martinez, California, who painted over a Black Lives Matter mural, have been charged with a hate crime."

The Wall Street Journal (7/7, Kusisto, Frosch, Subscription Publication) reports Floyd's death has also prompted the reexamination of older cases by local prosecutors.

New York City Police Arrest 195 In Fireworks Crackdown

WNBC-TV New York (7/7) reports, "Nearly 200 illegal fireworks have been made in New York City in the two weeks since Mayor Bill de Blasio unveiled a multi-agency task force to crack down on the problem amid an unprecedented level of complaints, officials said Tuesday." WNBC-TV adds, "The mayor revealed the task force, comprised of 10 officers with the NYPD Intelligence Bureau, 12 FDNY Fire Marshals and 20 Sheriff's Bureau of Criminal Investigation members, on June 23. Its primary goal: to disrupt illegal fireworks supply chains via sting operations within and outside New York City – and officials say the group busted a total of 195 people since it was established. It's not clear what prompted the extraordinary surge in illegal fireworks usage, which prompted sleep-deprived New Yorkers to protest in front of Gracie Mansion one night last month amid continued booming."

Protesters Charged With Leaking Police Document In Iowa

The AP (7/7, Foley) reports, "Prosecutors in Iowa have filed a rarely used leak charge against Black Lives Matter protesters accused of stealing a confidential police document and displaying it during a television news broadcast." The AP adds, "Two protesters are charged with unauthorized dissemination of intelligence data, a felony that carries up to five years in prison. The Iowa Judicial Branch says it's only the second time that the charge has been filed since 2010. It's intended to punish officers and others who share information that could undermine criminal investigations or violate privacy protections." According to the AP, "The document in question was a Des Moines Police Department bulletin that officers and state troopers had with them while patrolling a July 1 protest at the Iowa Capitol. The bulletin included photos of suspects who were wanted in the destruction of a Des Moines police car during a June 20 protest."

Dutch Police Arrest Six, Uncover Makeshift Torture Chamber

The AP (7/7, Corder) reports, "Dutch police arrested six men after discovering sea containers that had been converted into a makeshift prison and sound-proofed 'torture chamber' complete with a dentist's chair, tools including pliers and scalpels and handcuffs, a high ranking officer announced Tuesday. Authorities said police conducted the raid before the torture chamber could be used and alerted potential victims, who went into hiding." The AP adds, "The grisly discovery was made last month by officers investigating leads generated by data from encrypted phones used by criminals. The communications network was cracked recently by French police. Detectives in Britain and the Netherlands have already arrested hundreds of suspects based on the encrypted messages." According to the AP, "Tuesday's announcement gave a chilling insight into the increasingly violent Dutch criminal underworld, which is involved in the large scale production and trafficking of drugs."

TECHNOLOGY

German Authorities Seize Server Hosting "BlueLeaks" Data Dump

PCMag (7/7, Kan) reports, "German authorities have confiscated a server hosting the "BlueLeaks" data dump, a 269GB trove of internal police documents that leaked last month." According to PCMag, "The Wikileaks-style group Distributed Denial

of Secrets (DDOS) had been using the server to enable the public to download the files, but prosecutors in Germany recently seized it, according to Emma Best, a journalist and co-founder of the group. DDOS says it obtained the files from the 'hacktivist' collective Anonymous, and then made the files searchable on a dedicated website on July 19. However, the site now appears to be down." Best said "German authorities seized the 'primary public download server' hosting the data dump without supplying an explanation. The hosting provider has only said the takedown came from the 'department of public prosecution Zwickau,' which didn't immediately respond to a request for comment."

TUESDAY'S LEAD STORIES

- **Qualified Immunity At Forefront Of Policing Debate**
- **Door Of Portland, Oregon Federal Courthouse Shattered, Fireworks Exploded Inside**
- **New Mexico Militia Was Involved In June Shooting Incident In Albuquerque**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to theresa.olson@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Some US States Consider Police Licensing.

To:	Jennifer Warren (Sheriff)
Sent:	July 8, 2020 7:48:46 AM CDT
Received:	July 8, 2020 7:48:52 AM CDT

IACP's The Lead: Some US States Consider Police Licensing.

To:	Sean Gleason (Sheriff)
Sent:	July 8, 2020 7:48:46 AM CDT
Received:	July 8, 2020 7:48:50 AM CDT

[ISN] Cops Seize Server that Hosted BlueLeaks, DDoSecrets Says

From: InfoSec News <alerts@infosecnews.org>
To: isn@lists.infosecnews.org
Sender: ISN <isn-bounces@lists.infosecnews.org>

Sent: July 8, 2020 8:21:05 AM CDT
Received: July 8, 2020 8:27:22 AM CDT
Attachments: ATT00001.txt

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

https://www.vice.com/en_us/article/qj43xq/cops-seize-blueleaks-ddosecrets-server

By Lorenzo Franceschi-Bicchierai
Vice.com
July 7, 2020

Authorities in Germany have seized a server used by the organization that published a trove of US police internal documents commonly known as BlueLeaks, according to the organization's founder.

On Tuesday, Emma Best, the founder of Distributed Denial of Secrets or DDoSecrets, a WikiLeaks-like website that has published the police data, said that prosecutors in the German town of Zwickau seized the organization's "primary public download server."

"We are working to obtain additional information, but presume it is [regarding] #BlueLeaks," Best added on Twitter. "The server was used ONLY to distribute data to the public. It had no contact with sources and was involved in nothing more than enlightening the public through journalistic publishing."

Best shared a screenshot of the email they received from DDoSecrets' hosting provider informing of the server seizure.

[...]

[ISN] Cops Seize Server that Hosted BlueLeaks, DDoSecrets Says

To:	isn@lists.infosecnews.org, Christopher Moore (Sheriff), Keith Morrison (Sheriff), Patrick Kelly (Sheriff), Jonathan Springborn (Sheriff), Michael Aliperti, Ben Spear, bk@krebsonsecurity.com
Sent:	July 8, 2020 8:21:05 AM CDT
Received:	July 8, 2020 8:27:22 AM CDT

Your July Briefing

From: Information Management Today Monthly <editors@aggregage.com>
To: Keith Morrison <keith.morrison@cookcountyil.gov>, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: July 8, 2020 8:58:26 AM CDT
Received: July 8, 2020 8:58:37 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Top articles on Security and Military.

Edition : June, 2020

Information Management Today
Expert insights. Personalized for you.

Brought to you by

Trending Articles:

Future-Proofing Your Information Governance Strategy

Join Onna and experts from Quip, Airbnb, and Oracle for this recorded webinar as they dive into proactive data deletion policies, retention strategies, and legal hold practices that are essential to a modern enterprise information governance strategy.

ADVERTISER: ONNA

What Will Cybersecurity's 'New Normal' Look Like?

The coronavirus pandemic has forced changes for much of the business world, cybersecurity included. What can we expect going forward

DARK READING

How Covid-19 Contact Tracing Works on Your Phone

Developers are working on track-and-trace systems to keep infection levels low. The apps aren't here yet, but here's what they do—and how you can enable them. Gear Gear / How To and Advice Security

WIRED THREAT LEVEL

Attackers Target Vulnerable Exchange Servers

Microsoft Urges Patching, Other Mitigation Steps Microsoft is warning its customers that attackers are increasingly targeting unpatched Exchange servers, with a significant uptick in activity since April

Check out the full edition!

Picked For You:

Delivery Hero Confirms Foodora Data Breach

Personal Details on 727,000 Accounts in 14 Countries Leaked Delivery Hero, the online food delivery service, has confirmed a data breach of its Foodora brand. Breached information includes personal details for 727,000 accounts - names, addresses, phone numbers, precise location data and hashed passwords - in 14 countries

DATA BREACH TODAY

‘BlueLeaks’ Exposes Files from Hundreds of Police Departments

Hundreds of thousands of potentially sensitive files from police departments across the United States were leaked online last week. The collection, dubbed “ BlueLeaks ” and made searchable online, stems from a security breach at a Texas web design and hosting company that maintains a number of state law enforcement data-sharing portals.

KREBS ON SECURITY

MY TAKE: Remote classes, mobile computing heighten need for a security culture in K-12 schools

Parents have long held a special duty to protect their school-aged children from bad actors on the Internet. Related: Mock attacks help schools defend themselves Now COVID-19 has dramatically and permanently expanded that parental responsibility, as well as extended it to ill-prepared school officials in K-12 campuses all across the nation.

THE LAST WATCHDOG

More Trending:

Anonymous Stole and Leaked a Megatrove of Police Documents

The so-called BlueLeaks collection includes internal memos, financial records, and more from over 200 state, local, and federal agencies. Security Security / Cyberattacks and Hacks

WIRED THREAT LEVEL

City Pays Ransom Despite Pre-Ransomware Outbreak Hack Alert

DoppelPaymer Hit Comes as Ransomware Attacks - and Data-Leaking Shakedowns - Surge The attack sounds ripped from an episode of TV show "24": Hackers have infiltrated a government network, and they're days away from unleashing ransomware.

DATA BREACH TODAY

Google Removes More Than 70 Malicious Chrome Extensions

Researchers Find Extensions Could Steal Credentials and Security Tokens Google has removed more than 70 malicious Chrome extensions after researchers with security firm Awake Security discovered the extensions could be used to steal users' credentials and security tokens

DATA BREACH TODAY

Click here to see this edition in full, including:

Dating Apps Exposed 845GB of Explicit Photos, Chats, and More
WIRED THREAT LEVEL

How to keep your remote work team together
OPENTEXT INFORMATION MANAGEMENT

7 Ransomware Trends: Gangs Join Forces, Decryptors Improve
DATA BREACH TODAY

Turn on MFA Before Crooks Do It For You
KREBS ON SECURITY

Hundreds of malicious Chrome browser extensions used to spy on you!
SECURITY AFFAIRS

Good Cyber Hygiene in a Post-Pandemic World Starts with Us
DARK READING

Even Ethical Hackers Abuse Cloud Services
DATA BREACH TODAY

Facebook and Twitter Want to Keep the Justice System Skewed Against Defendants

WIRED THREAT LEVEL

79 Netgear router models affected by a dangerous Zero-day

SECURITY AFFAIRS

Bank Card "Master Key" Stolen

SCHNEIER ON SECURITY

Check out the full edition!

Copyright 2020 | Aggregage | 525 South Douglas Ave, Suite 260 | El Segundo, CA 90245 USA. Email sent to keith.morrison@cookcountyil.gov. To stop receiving emails at this address manage your subscription or unsubscribe. Powered by Aggregage - expert insights. personalized for you.. Forward this email to a friend!

<!

The CyberWire 7.8.20: Natanz blast looks more like a bomb than a cyber-induced failure. CISA announces ICS strategy. FBI Director on cyberespionage.

From: The CyberWire <editor@thecyberwire.com>

To: Keith.Morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: July 8, 2020 10:32:43 AM CDT

Received: July 8, 2020 10:33:07 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

More signal, less noise.

SPONSORED BY LOOKINGGLASS CYBER SOLUTIONS:

Lure & Deceive: Using Deception Technology to Defeat your Adversary

Staying one step ahead of your adversaries is more challenging than ever. Fortunately, deception technology can give new visibility and intelligence in combating threat actors who seek to infiltrate your network.

View our on-demand webinar to learn how to optimize your deception technology investments to enhance your day-to-day security threat detection and mitigation activities.

Daily briefing.

July 8, 2020.

SUMMARY

By the CyberWire staff

It appears increasingly likely that the explosion at Iran's Natanz nuclear facility was sabotage, and not a cyberattack (EurAsian Times has a summary of the emerging consensus). The connections, if any, between the Natanz incident and damage recently worked elsewhere in Iran remain unclear, Haaretz notes, but it does seem that Iran's nuclear program figures on some adversary's target list.

The US Cybersecurity and Infrastructure Security Agency (CISA) yesterday released its strategy document, Securing Industrial Control Systems: A Unified Initiative.

At a speech before the Hudson Institute yesterday, US FBI Director Wray denounced Chinese intelligence operations as, according to Axios, serving Beijing's ambitions to become the world's dominant power. CNBC's coverage of the speech concentrated on Director Wray's account of Chinese industrial espionage.

Vice reports that police in Zwickau, Saxony, seized the server used by DDoSecrets, aspiring successor to WikiLeaks. DDoSecrets doesn't know why the server was taken, but assumes the seizure was due to the group's BlueLeaks program of doxing US police departments.

Bloomberg Law reports that Mexico's central bank sustained but successfully parried a cyberattack yesterday. Banco de México said that the denial-of-service attempt lasted about half an hour and caused brief, intermittent outages before it was finally stopped, and service returned to normal.

EDP Renewables North America, a renewable energy subsidiary of Energias de Portugal, has disclosed a databreach. The company characterizes it as unauthorized intrusion into its networks, but says it believes no customer data were compromised. SecurityWeek calls the incident a Ragnar Locker ransomware infection.

[250]

SPONSORED BY GDIT:

Secure your mission with the GDIT Cyber Stack, our ecosystem of cyber capabilities.

Notes.

Today's issue includes events affecting Brazil, China, France, Germany, India, Mexico, Russia, the United Arab Emirates, and the United States.

Word Notes Wednesday.

copy-paste compromise (Noun): Successful breaches accomplished using only open-source tools. The adversary uses no original code to traverse the intrusion kill chain.

Aerospace news worthy of attention.

If you're interested in space and communications (technology, policy, business, and operations), take a look at the latest issue of Cosmic AES Signals & Space. Produced in partnership with the CyberWire, Signals & Space offers a monthly overview of news in this sector.

SPONSORED BY FIREEYE:

Available Now: Mandiant Security Effectiveness Report 2020

Government agencies are the third most targeted industry by threat actors. In order to be prepared for cyber incidents, they need tools to measure their security effectiveness so they can understand & manage their cyber risks. The Security Effectiveness Report 2020 gives you a detailed look at these threats and how you combat this reality.

ON THE PODCAST

In today's CyberWire Daily Podcast, out later this afternoon, we speak with our partners at the Johns Hopkins University's Information Security Institute, as Joe Carrigan talks about personal privacy measures for iOS and Android. Our guest, Steve Moore from Exabeam, has spent a good year interviewing CISOs, and he shares what he's learned from his interlocutors.

And Caveat is up. In this week's episode, "Huawei statements are not as strong as before," Dave's got the story of a school district in hot water over facial recognition issues, Ben has the story of protesters being tracked via their mobile devices, and later in the show our conversation with Shannon Vavra with CyberScoop on her recent article, "Huawei execs admit they don't know whether their tech is used for surveillance."

SPONSORED EVENTS

OSINT Insiders: The Rise and Evolution of Open Source Intelligence (Online, July 10, 2020) Join OSINT Insiders live on Friday, July 10! Major General (Retired) Mark R. Quantock of Babel Street will share his perspective on the rise of Open Source Intelligence (OSINT) and how it has evolved over the years.

Cyber Security Summit Virtual Power Hour - Get the Facts on July 14 and 16 (Online, July 14 - 16, 2020) Senior Level Executives are invited to the upcoming Cyber Summit Virtual Power Hours. Learn from Industry Experts from The FBI, U.S. Secret Service, U.S. DHS, Google, IBM Security, KnowBe4 & Duo Security as they discuss the latest security challenges & develop cyber security battle plans in today’s unprecedented times. You will receive 1 CPE / CEU credit by attending. Free to register with code: CyberWire20 at CyberSummitUSA.com.

IoT Integrator Summit: Securing Edge Computing (Online, July 14 - 16, 2020) A virtual summit to help IoT Integrators learn more about advances and updates in IoT security and

discover new methods for architecting IoT solutions for your organization or your clients.

RSA Conference APJ July 15-17, 2020 - A Virtual Learning Experience (Online, July 15 - 17, 2020) The world's leading cybersecurity event is going virtual 15-17 July. Join your peers and industry experts for three days of insights. Watch over 50 sessions live during Singapore business hours—or stream them later. Register today for free.

SELECTED READING

Cyber Attacks, Threats, and Vulnerabilities

Attack On Iran's Natanz Nuclear Facility Not A Cyber Attack, But A Bomb Blast – Reports (EurAsian Times) The recent explosion at Natanz nuclear facility in Iran has set back its nuclear program by more than...

Experts: Natanz explosion set back Iran's nuclear program by more than a year (Haaretz) It's unclear if the explosion and other incidents that occurred in Iran over the past week were connected,...

Mexico's Central Bank Thwarts Cyber Attack on Its Website (Bloomberg Law) Mexico's central bank said it thwarted a cyberattack on its website Tuesday, although its web page had...

Find MORE on our website.

Security Patches, Mitigations, and Software Updates

New round of bugs found in Citrix software, but this time a patch is ready (CyberScoop) On Tuesday, Citrix revealed 11 new vulnerabilities in its cloud-based and remote access products, ADC...

Citrix tells everyone not to worry too much over its latest security patches. NSA's former top hacker disagrees (Register) Eleven flaws cleaned up including one that may be exploited to sling malware downloads

Mozilla turns off "Firefox Send" following malware abuse reports (Naked Security) Sadly, the easier and safer you make your file sharing service, the more attractive it becomes to the...

Find MORE on our website.

Cyber Trends

Bitglass 2020 BYOD Report: Increased Remote Work Drives BYOD, but Security is Not Keeping Pace (BusinessWire) Bitglass, the Total Cloud Security company, has released its 2020 BYOD Report, which analyzes enterprise...

M&D Report (Sikich LLP) M&D Report 2019 Sikich's fifth Manufacturing & Distribution survey was recently completed—and the results...

Physical stress to phishing: Real challenges of virtual gaming and how to counter them

(Firstpost) The rapidly-growing Esports industry has its own issues that manifest in the form of various risks associated...

Marketplace

Tech Startups Hemorrhaging Jobs During Pandemic (Channel Futures) A new BuyShares report shows tech startups have been heavily impacted by the COVID-19 pandemic, with...

Thoma Bravo acquires Exostar (PE Hub) Thoma Bravo has acquired Exostar LLC, a provider of secure business collaboration solutions.

QOMPLX announces plans for US insurance subsidiary RubiQon Risk/RubiQon Re (PR Newswire) QOMPLX™, an intelligent decision platform provider, today announced the launch of a US-based subsidiary...

Find MORE on our website.

Products, Services, and Solutions

iProov Provides Online Biometric Safeguarding for Intergenerational Mentoring Platform, bloomd (BusinessWire) iProov, world-leaders in spoof-resistant biometric authentication technology, is continuing to provide...

Bricata Partners with Elastic to Deliver Comprehensive Network Securit (PRWeb) Bricata, Inc., a leading provider of comprehensive network protection, today announced a technology partnership...

New F5 Solution Defends Customers' Websites through Protection against Bots and Credential Stuffing (BusinessWire) F5 (NASDAQ: FFIV) today unveiled Silverline Shape Defense, a security solution that protects websites...

Find MORE on our website.

Technologies, Techniques, and Standards

Cyber Command will get a new version of its training platform this fall (C4ISRNET) The Persistent Cyber Training Environment is slated to deliver its second version to the cyber mission...

Marine Corps activates new battalion to fight in cyberspace (Camp Lejeune Globe) An impactful change to Marine Corps cyberspace and information technology modernization occurred June...

Adopt These Video Conferencing Security Best Practices to Strengthen Your Digital Security (Security Intelligence) Video conferencing use spiked during COVID-19 due to remote work, but security risks were likely overlooked.

Design and Innovation

Scrutiny is key to the success of digital immunity passports (Computing) Is the convenience of a digital coronavirus immunity document worth the privacy concerns and

investment,...

Hardware enclaves - the next frontier in enterprise application security (diginomica) Hardware enclaves - security's next big thing.

Research and Development

Ben-Gurion University researchers determine how to accurately pinpoint malicious drone operators (EurekAlert!) When tested in simulated drone paths, the model was able to predict the operator location with 78% accuracy.

Academia

NSA designates Wright State center for cyber defense education (Dayton Daily News) Wright State University has won a federal designation as a go-to center for cyber defense education.

Legislation, Policy, and Regulation

China's Second Wave of Coronavirus Censorship Is Here (Foreign Policy) After a brief period of praising whistleblowers, Beijing is targeting medical staff and COVID-19 victims...

In Hong Kong National Security Law, Echoes of China's Own Cyber Crackdown (New York Times) Hong Kong's new National Security Law will shake up digital surveillance in the city, with strict new...

China aims to dominate everything from 5G to AI (CNET) Generation China is a CNET series looking at how the country is staking out positions in the biggest...

Find MORE on our website.

Litigation, Investigation, and Law Enforcement

Exclusive: U.S. probing allegations TikTok violated children's privacy - sources (Reuters) The Federal Trade Commission and the U.S. Justice Department are looking into allegations that popular...

Russia Arrests Space Agency Official, Accusing Him of Treason (New York Times) The detention of Ivan Safronov, a former journalist who had been working as an adviser at Roscosmos,...

Lawmakers paralyzed over response to Russian bounty intel (POLITICO) Trump has called initial reporting on the bounties a hoax.

Find MORE on our website.

INDUSTRY EVENTS

For a complete running list of events, please visit the Event Tracker on the CyberWire

website.

Newly Noted Events

The Future of Digital Engagement Is Here (Online, July 29, 2020) Businesses are facing a period of complex global change and disruption. What's on the horizon? Akamai...

Upcoming Events

WSIS Forum 2020 (Online, June 22 - September 10, 2020) The World Summit on the Information Society (WSIS) Forum 2020, celebrates 15 years of providing a multi-stakeholder...

Inaugural Toronto Cyber Security Summit (Toronto, Ontario, Canada, July 14, 2020) C-Suite & Senior Level Executives: Register with Promo Code CYBERWIRE95 to receive $95 Admission (Standard...

SecureWorld Boston 2020 Virtual Conference (Online, July 15, 2020) Join the cybersecurity community for high-quality training and collaboration through an interactive online...

7th Annual DC Metro Cyber Security Summit (McLean, Virginia, USA, July 23, 2020) C-Suite & Senior Level Executives: Register with Promo Code CYBERWIRE95 to receive $95 Admission (Standard...

SecureWorld New York - Philadelphia Virtual Conference 2020 (Online, July 29, 2020) Join the cybersecurity community for high-quality training and collaboration through an interactive online...

SPONSOR & SUPPORT

Grow your brand and reach new customers.

Grow your brand and increase your customer base by educating our audience about your products, services, and events by advertising on The CyberWire. We've built trust with an influential (and often hard to reach) audience of CISOs, CSOs, and other senior execs in the security space, across a wide array of industry verticals. Learn more.





Copyright © 2020, CyberWire Inc. Views and assertions of the various sources cited, Selected Reading articles, and cartoons are those of the authors and artists, not the CyberWire, Inc.

This email was sent to Keith.Morrison@cookcountyil.gov
why did I get this? | unsubscribe | update subscription preferences

The CyberWire · 8110 Maple Lawn Blvd. · Suite 200 · Fulton, Md 20759 · USA

ISN Digest, Vol 53, Issue 5

From: isn-request@lists.infosecnews.org
To: isn@lists.infosecnews.org
Sender: ISN <isn-bounces@lists.infosecnews.org>
Sent: July 8, 2020 11:00:03 AM CDT
Received: July 8, 2020 11:00:28 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

Send ISN mailing list submissions to
isn@lists.infosecnews.org

To subscribe or unsubscribe via the World Wide Web, visit
http://lists.infosecnews.org/mailman/listinfo/isn_lists.infosecnews.org

or, via email, send a message with subject or body 'help' to
isn-request@lists.infosecnews.org

You can reach the person managing the list at
isn-owner@lists.infosecnews.org

When replying, please edit your Subject line so it is more specific
than "Re: Contents of ISN digest..."

Today's Topics:

1. Energy company EDP confirms cyberattack, Ragnar Locker
ransomware blamed (InfoSec News)
2. Cops Seize Server that Hosted BlueLeaks, DDoSecrets Says
(InfoSec News)
3. Today is the Day I have Dreaded for the Last 5 Years
(InfoSec News)
4. Citrix patches 11 critical bugs (InfoSec News)
5. Magellan Health Data Breach Victim Tally Reaches 365K
Patients (InfoSec News)
6. Looks Like Russian Hackers Are on an Email Scam Spree
(InfoSec News)
7. Customer data from fitness firm V Shred exposed on
misconfigured cloud storage (InfoSec News)

Message: 1
Date: Wed, 8 Jul 2020 13:14:27 +0000 (UTC)
From: InfoSec News <alerts@infosecnews.org>
To: isn@lists.infosecnews.org
Subject: [ISN] Energy company EDP confirms cyberattack, Ragnar Locker

ransomware blamed
Message-ID:
<alpine.DEB.2.21.2007081313170.11119@ip-172-30-0-239.ec2.internal>
Content-Type: text/plain; format=flowed; charset=US-ASCII

https://www.zdnet.com/article/edp-energy-confirms-cyberattack-ragnar-locker-ransomware-blamed/

By Charlie Osborne
Zero Day
ZDNet.com
July 7, 2020

EDP Renewables North America (EDPR NA) has disclosed a cyberattack in which ransomware landed on parent company Energias de Portugal (EDP)'s systems, potentially leading to information exposure.

In a letter sent to customers (.PDF), the energy company apologized for the incident but insisted that there is "no evidence" that consumer information was compromised or stolen.

The firm delivers energy to over 11 million customers and operates in 19 countries.

EDP experienced a ransomware attack on April 13. EDPR NA learned of the ransomware infection "for the first time" from its parent company on May 8.

[...]

Message: 2
Date: Wed, 8 Jul 2020 13:21:05 +0000 (UTC)
From: InfoSec News <alerts@infosecnews.org>
To: isn@lists.infosecnews.org
Subject: [ISN] Cops Seize Server that Hosted BlueLeaks, DDoSecrets Says
Message-ID:
<alpine.DEB.2.21.2007081320540.11119@ip-172-30-0-239.ec2.internal>
Content-Type: text/plain; charset="utf-8"; Format="flowed"

https://www.vice.com/en_us/article/qj43xq/cops-seize-blueleaks-ddosecrets-server

By Lorenzo Franceschi-Bicchierai
Vice.com
July 7, 2020

Authorities in Germany have seized a server used by the organization that published a trove of US police internal documents commonly known as BlueLeaks, according to the organization?s founder.

On Tuesday, Emma Best, the founder of Distributed Denial of Secrets or DDoSecrets, a WikiLeaks-like website that has published the police data, said that prosecutors in the German town of Zwickau seized the organization?s ?primary public download server.?

?We are working to obtain additional information, but presume it is [regarding] #BlueLeaks,? Best added on Twitter. ?The server was used ONLY to distribute data to the public. It had no contact with sources and was involved in nothing more than enlightening the public through journalistic publishing.?

Best shared a screenshot of the email they received from DDoSecrets? hosting provider informing of the server seizure.

[...]

Message: 3
Date: Wed, 8 Jul 2020 13:21:23 +0000 (UTC)
From: InfoSec News <alerts@infosecnews.org>
To: isn@lists.infosecnews.org
Subject: [ISN] Today is the Day I have Dreaded for the Last 5 Years
Message-ID:
<alpine.DEB.2.21.2007081321110.11119@ip-172-30-0-239.ec2.internal>
Content-Type: text/plain; charset="utf-8"; Format="flowed"

https://medium.com/@iHeartMalware/today-is-the-day-i-have-dreaded-for-the-last-5-years-51db99ee38fa

Ronnie T
Jul 7, 2020

September 2015 is when it all started. At the time I was working at PhishMe (now Cofense), and our CFO received a shady looking email, asking if he was busy.

?I have no idea what this is, can you guys take a look at it? Rohyt didn?t send this email.?

Aaron and I started looking at the email to figure out what was going on. At the time emails never needed a response, because malicious emails were just that: malicious, and always contained malware. This one was a little different, as there was no malware to be found. Where?s the macro or link? Where?s the payload? My handle is literally ?iHeartMalware?, but there?s no way to infect a user with this. It?s just someone asking fo-AH HA!

The email wanted our CFO to do a wire transfer, but we were still lacking context. Why did they want a wire transfer? Aaron suggest responding back to the scammers to see how it played out, and we did. Without missing a beat the scammers responded, sent a bank account, and asked for us to transfer money to an account under their control. We published the research, and even referenced the FBI statistics of 2015 from Mr. Brian Krebs himself, FBI lost 1.2 billion

dollars to Business Email Scams. OMG, a billion dollars? That?s a lot of money being lost, and we should probably start trying to figure this out.

Current me is looking back at past me:

The more we studied this new thing called business email compromise, the worse it got. We started working with other private companies to try and understand the problem, and that?s when the BEC mailing list was born. Christmas of 2015. Initially we were 100 security professionals and 10 FBI agents, and our goal was that: to study and begin to understand how this BEC mess worked. Everything was held at the TLP:Red level as a way to ensure that information could be shared freely and securely, and collaboration worked. It worked really well. 110 people, we got this, right? ?Right?

3.1 billion.

[...]

Message: 4
Date: Wed, 8 Jul 2020 13:21:37 +0000 (UTC)
From: InfoSec News <alerts@infosecnews.org>
To: isn@lists.infosecnews.org
Subject: [ISN] Citrix patches 11 critical bugs
Message-ID:
<alpine.DEB.2.21.2007081321260.11119@ip-172-30-0-239.ec2.internal>
Content-Type: text/plain; charset="utf-8"; Format="flowed"

https://www.infosecnews.org/citrix-patches-11-critical-bugs/

By William Knowles @c4i
Senior Editor
InfoSec News
July 8, 2020

In a breath of fresh air for this week, software vendor Citrix released patches for 11 vulnerabilities, quickly applying the lesson learned six months ago and not wanting a repeat with malicious hackers looking for ways to exploit the vulnerability.

Citrix Chief Information Security Officer, Fermin J. Serna released a bulletin on Tuesday, July 7, which covered a set of vulnerabilities in Citrix?s products? Citrix ADC, Citrix Gateway, and Citrix SD-WAN WANOP edition. Standard procedure for most software companies in advising customers of vulnerabilities is limited to the publication of the bulletin and related CVEs.

Serna took the opportunity to explain the following points as it relates to CTX276688.

[...]

Message: 5
Date: Wed, 8 Jul 2020 13:22:08 +0000 (UTC)
From: InfoSec News <alerts@infosecnews.org>
To: isn@lists.infosecnews.org
Subject: [ISN] Magellan Health Data Breach Victim Tally Reaches 365K Patients
Message-ID: <alpine.DEB.2.21.2007081321570.11119@ip-172-30-0-239.ec2.internal>
Content-Type: text/plain; charset=US-ASCII; format=flowed

https://healthitsecurity.com/news/magellan-health-data-breach-victim-tally-reaches-365k-patients

By Jessica Davis
Health IT Security.com
July 7, 2020

July 07, 2020 - The extent of the ransomware attack that hit Arizona-based Magellan Health in April became clear this week, with eight Magellan Health affiliates and healthcare providers reporting breaches stemming from the incident to the Department of Health and Human Services. The breach reporting tools shows about 365,000 patients were affected.

In April, the Fortune 500 company was reportedly the victim of a sophisticated cyberattack, in which hackers first exfiltrated data before deploying the ransomware payload. By leveraging a social engineering phishing scheme that impersonated a Magellan client, the attackers were able to gain access to the system five days before the ransomware attack.

The investigation determined hackers first installed malware able to steal employee credentials and passwords to gain access to the affected server. Patient data was also compromised in the event, including health-related information such as health insurance account data and treatment information.

The attack was contained to a single corporate server, which compromised the data of current employees and a trove of sensitive patient data, from Social Security numbers and W-2 information, to taxpayer identification and employee ID numbers.

[...]

Message: 6
Date: Wed, 8 Jul 2020 13:22:13 +0000 (UTC)
From: InfoSec News <alerts@infosecnews.org>
To: isn@lists.infosecnews.org
Subject: [ISN] Looks Like Russian Hackers Are on an Email Scam Spree
Message-ID:

<alpine.DEB.2.21.2007081319100.11119@ip-172-30-0-239.ec2.internal>
Content-Type: text/plain; charset="utf-8"; Format="flowed"

https://www.wired.com/story/russian-hackers-email-scams/

By Lily Hay Newman
Security
Wired.com
July 7, 2020

FOR YEARS, COSTLY email grifts have largely been the provenance of West African scammers, particularly those based in Nigeria. A newly discovered "business email compromise" campaign, though, appears to come from a criminal group in a part of the world better known for a different brand of online mayhem: Russia.

Dubbed Cosmic Lynx, the group has carried out more than 200 BEC campaigns since July 2019, according to researchers from the email security firm Agari, particularly targeting senior executives at large organizations and corporations in 46 countries. Cosmic Lynx specializes in topical, tailored scams related to mergers and acquisitions; the group typically requests hundreds of thousands or even millions of dollars as part of its hustles. The researchers, who have worked extensively on tracking Nigerian BEC scammers, say they don't have a clear sense of how often Cosmic Lynx actually succeeds at obtaining a payout. Given that the group hasn't lowered its asks in a year, though, and has been prolific about developing new campaigns?including some compelling Covid-19?related scams?Agari reasons that Cosmic Lynx must be raking in a fair amount of money.

"Most Eastern European and Russian hackers have been so entrenched in malware campaigns and technically sophisticated infrastructure that, as long as there are returns, they don?t need to adapt," says Crane Hassold, senior director of threat research at Agari and a former digital behavior analyst for the Federal Bureau of Investigation. "But defenses against technically sophisticated attacks have gotten significantly better, and they're realizing that the return on investment for these social-engineering-based attacks is much higher."

West African scammers typically run their BEC campaigns off of rented or free cloud infrastructure using free email accounts. They have increasingly branched out into utilizing off-the-shelf hacking tools like keyloggers and even backdoors into targets' systems, but malware has typically not played a major role. Overhead is much lower when you don't need to develop and maintain your own infrastructure and software. This may have been a selling point for Cosmic Lynx, which combines some of the technical chops of a Russian criminal hacking group with the cost savings of a classic, low-tech BEC attack.

[...]

Message: 7
Date: Wed, 8 Jul 2020 13:21:54 +0000 (UTC)
From: InfoSec News <alerts@infosecnews.org>
To: isn@lists.infosecnews.org
Subject: [ISN] Customer data from fitness firm V Shred exposed on
misconfigured cloud storage
Message-ID:
<alpine.DEB.2.21.2007081321430.11119@ip-172-30-0-239.ec2.internal>
Content-Type: text/plain; charset="utf-8"; Format="flowed"

https://siliconangle.com/2020/07/02/customer-data-fitness-company-v-shred-exposed-misconfigured-cloud-storage/

By Duncan Riley
SiliconAngle.com
July 2, 2020

Data relating to at least 99,000 customers of fitness company V Shred LLC has been exposed online in yet another case of misconfigured cloud storage.

Discovered by security researchers Noam Rotem and Ran Locar at vpnMentor and reported today, the unsecured data was found in an Amazon Web Services Inc. S3 bucket. The data, which came in at a sizable 606 gigabytes, included about 1.3 million files relating to V Shred customers.

The database included full names, home addresses, email addresses, phone numbers, birthdays, Social Security numbers, spouse names, social media accounts, gender, health conditions, age range, citizenship status, usernames and passwords. The database also included account profile photos, ?revealing? before and after photos and custom meal plans.

The exposed database was discovered on May 14, with V Shred contacted May 18. After no response from the company, the researchers then contacted AWS May 20. AWS responded June 1 and the database was taken offline June 18.

[...]

Subject: Digest Footer

--
Subscribe to InfoSec News
https://www.infosecnews.org/subscribe-to-infosec-news/
Follow InfoSec News on Twitter
https://twitter.com/infosecnews_
Follow InfoSec News on LinkedIn
https://www.linkedin.com/company/infosecnews/

End of ISN Digest, Vol 53, Issue 5

Fw: IACP's The Lead: Some US States Consider Police Licensing.

From: Sean Gleason (Sheriff) <Sean.Gleason@cookcountyil.gov>
To: 2020 Criminal Investigations Supervisors <2020CriminalInvestigationsSupervisors@cookcounty.onmicrosoft.com>
Sent: July 8, 2020 1:11:54 PM CDT
Received: July 8, 2020 1:11:55 PM CDT

Sean M. Gleason
Commander
Criminal Investigations Section
Cook County Sheriff's Police Department
1401 South Maybrook Drive
Maywood, Illinois 60153
Work Phone: 708/865-4801

From: The IACP <TheLead@iacp.bulletinmedia.com>
Sent: Wednesday, July 8, 2020 7:48 AM
To: Sean Gleason (Sheriff) <Sean.Gleason@cookcountyil.gov>
Subject: IACP's The Lead: Some US States Consider Police Licensing.

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Sean Gleason

Wednesday, July 8, 2020

POLICING & POLICY

Some US States Consider Police Licensing

Bloomberg Law (7/7, Ebert, Subscription Publication) reports, "Government officials in at least a half-dozen states want to make it easier to end the policing careers of abusive officers by making it hard for them to start fresh in new jurisdictions. 'Now is the time, I believe, to begin treating peace officer certificates more like licenses,' said Ohio Gov. Mike DeWine. 'The only way the state can revoke a peace officer certificate today is if that officer is convicted of a felony,' he said in unveiling a proposal to beef up statewide oversight of law enforcement. 'There is no mechanism in Ohio to revoke a certificate for conduct that might be bad, might be horrible, but is not necessarily criminal.'" Bloomberg Law adds, "Occupational licensing proposals for law enforcement have been pitched in recent weeks in California, Illinois, Massachusetts, New Jersey, Ohio, and Michigan. Three of those states – California, Massachusetts, and New Jersey – along with Rhode Island lack any statewide procedure for decertifying officers."

San Diego, California To Put Police Reform Measure On November Ballot

The San Diego Union-Tribune (7/7, Garrick) reports, "Critics of local law enforcement got a key win Tuesday when the San Diego City Council unanimously agreed to place a long-awaited police reform measure on the November ballot." According to the Union-Tribune, "City voters will get a chance this November to create a new police oversight board that would have the power to launch independent misconduct investigations, subpoena witnesses and hold officers more accountable for their actions. Community leaders and council members said Tuesday's vote was an important milestone that would allow voters to boost transparency and accountability for local police. But they also stressed that much more needs to be done on police reform." The Union-Tribune adds, "Other recent reform efforts in San Diego include a ban on police officers using carotid restraints, new Police Department de-escalation procedures and creation of an Office on Race and Equity."

US House Democrats Include $597 Million For Police Reform In Spending Bill

The Hill (7/7, Elis) reports, "House Democrats included a slew of police reforms, as well as $596.7 million in funding for reform programs, in a proposed spending bill for the 2021 fiscal year, which begins in October." The Hill adds, "The 2021 Commerce, Justice, Science appropriations bill includes $400 million for initiatives that would boost independent investigations of law enforcement, pattern and practice investigations that look for systemic problems in policing, community-based organizations seeking to improve law enforcement and other initiatives. It would also provide $50 million to train local law enforcement on certain best practices, $77.5 million to grant programs to boost police-community relations, $25 million for federal investigations into misconduct and $4 million for civilian review boards."

US Lawmakers Unveil Bill To Defund Police, Provide Reparations

The New York Post (7/7, Nelson) reports that US Reps. Ayanna Pressley (D-MA) and Rashida Tlaib (D-MI) on Tuesday "announced federal legislation to defund police and set up reparations for people who either are black or were harmed by cops." The two lawmakers announced the measure "on a Zoom call," but it "has not yet been introduced." Said Tlaib, "We can start to envision through this bill a new version for public safety – a new vision for public safety, one that protects and affirms Black lives."

The AP (7/7, Stafford) reports, "Dubbed the BREATHE Act, the legislation is the culmination of a project led by the policy table of the Movement for Black Lives, a coalition of more than 150 organizations."

Minnesota Lawmakers Remain Hopeful About Police Reform Efforts

The Minneapolis Star Tribune (7/8, Berkel, Bierschbach) reports, "Minnesota state lawmakers will get another chance at passing police accountability measures into law next week, with Gov. Tim Walz planning to call a special legislative session for the second time this summer." The Star Tribune adds, "Walz said Tuesday he is optimistic that lawmakers can strike a deal on both a public works spending package and on police reforms in the wake of the May death of George Floyd at the hands of

Minneapolis police officers." House Democrats "continue to push for a sweeping package of changes to boost community-led alternatives to policing, ban warrior-style training for officers and raise the threshold for using deadly force from 'apparent' to 'imminent' threats to officers and others."

For U.S. Members:
The 2019–2020 Public Safety Officer Medal of Valor is the United States' highest public safety honor that can be awarded to law enforcement officers, emergency medical personnel, and firefighters. This award honors federal, state, local, and tribal public safety officers who have demonstrated exceptional bravery, risking serious injury or death, in the line of duty. The Bureau of Justice Assistance is seeking nominations for the Medal of Valor now through **Friday, July 31, 2020.**
Public Safety Officers can be nominated for any qualifying event between June 1, 2019, and May 31, 2020. Public Safety Officers must be nominated by the heads of their agencies by July 31, 2020, at 11:59 p.m. ET to be considered for this award. Agency heads may submit multiple nominations to honor several officers or to honor one officer for multiple separate events. Nomination guidelines and stories of past recipients can be found on the Medal of Valor website.

Connect with the IACP online: **IACP Event Calendar:**

CRIME & DRUGS

Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests

USA Today (7/7, Philimon) reports that a "range of disturbing incidents have happened since George Floyd's death and subsequent protests against racism and police brutality." In Illinois, for example, "a man was charged with a hate crime for allegedly riding his motorcycle into a protest and hitting two people," and "authorities say a KKK leader tried to run his car through a group of peaceful protesters in Virginia."

The Washington Examiner (7/7, Smith), meanwhile, reports that "two white residents of Martinez, California, who painted over a Black Lives Matter mural, have been charged with a hate crime."

The Wall Street Journal (7/7, Kusisto, Frosch, Subscription Publication) reports Floyd's death has also prompted the reexamination of older cases by local prosecutors.

New York City Police Arrest 195 In Fireworks Crackdown

WNBC-TV New York (7/7) reports, "Nearly 200 illegal fireworks have been made in New York City in the two weeks since Mayor Bill de Blasio unveiled a multi-agency task force to crack down on the problem amid an unprecedented level of complaints, officials said Tuesday." WNBC-TV adds, "The mayor revealed the task force, comprised of 10 officers with the NYPD Intelligence Bureau, 12 FDNY Fire Marshals and 20 Sheriff's Bureau of Criminal Investigation members, on June 23. Its primary goal: to disrupt illegal fireworks supply chains via sting operations within and outside New York City – and officials say the group busted a total of 195 people since it was established. It's not clear what prompted the extraordinary surge in illegal fireworks usage, which prompted sleep-deprived New Yorkers to protest in front of Gracie Mansion one night last month amid continued booming."

Protesters Charged With Leaking Police Document In Iowa

The AP (7/7, Foley) reports, "Prosecutors in Iowa have filed a rarely used leak charge against Black Lives Matter protesters accused of stealing a confidential police document and displaying it during a television news broadcast." The AP adds, "Two protesters are charged with unauthorized dissemination of intelligence data, a felony that carries up to five years in prison. The Iowa Judicial Branch says it's only the second time that the charge has been filed since 2010. It's intended to punish officers and

others who share information that could undermine criminal investigations or violate privacy protections." According to the AP, "The document in question was a Des Moines Police Department bulletin that officers and state troopers had with them while patrolling a July 1 protest at the Iowa Capitol. The bulletin included photos of suspects who were wanted in the destruction of a Des Moines police car during a June 20 protest."

Dutch Police Arrest Six, Uncover Makeshift Torture Chamber

The AP (7/7, Corder) reports, "Dutch police arrested six men after discovering sea containers that had been converted into a makeshift prison and sound-proofed 'torture chamber' complete with a dentist's chair, tools including pliers and scalpels and handcuffs, a high ranking officer announced Tuesday. Authorities said police conducted the raid before the torture chamber could be used and alerted potential victims, who went into hiding." The AP adds, "The grisly discovery was made last month by officers investigating leads generated by data from encrypted phones used by criminals. The communications network was cracked recently by French police. Detectives in Britain and the Netherlands have already arrested hundreds of suspects based on the encrypted messages." According to the AP, "Tuesday's announcement gave a chilling insight into the increasingly violent Dutch criminal underworld, which is involved in the large scale production and trafficking of drugs."

TECHNOLOGY

German Authorities Seize Server Hosting "BlueLeaks" Data Dump

PCMag (7/7, Kan) reports, "German authorities have confiscated a server hosting the "BlueLeaks" data dump, a 269GB trove of internal police documents that leaked last month." According to PCMag, "The Wikileaks-style group Distributed Denial of Secrets (DDOS) had been using the server to enable the public to download the files, but prosecutors in Germany recently seized it, according to Emma Best, a journalist and co-founder of the group. DDOS says it obtained the files from the 'hacktivist' collective Anonymous, and then made the files searchable on a dedicated website on July 19. However, the site now appears to be down." Best said "German authorities seized the 'primary public download server' hosting the data dump without supplying an explanation. The hosting provider has only said the takedown came from the 'department of public prosecution Zwickau,' which didn't immediately respond to a request for comment."

TUESDAY'S LEAD STORIES

- **Qualified Immunity At Forefront Of Policing Debate**
- **Door Of Portland, Oregon Federal Courthouse Shattered, Fireworks Exploded Inside**
- **New Mexico Militia Was Involved In June Shooting Incident In Albuquerque**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to sean.gleason@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

Fw: IACP's The Lead: Some US States Consider Police Licensing.

To: 2020 Criminal Investigations Supervisors, Scott Lefko (Sheriff)
Sent: July 8, 2020 1:11:54 PM CDT
Received: July 8, 2020 1:11:56 PM CDT

Fw: IACP's The Lead: Some US States Consider Police Licensing.

To:	2020 Criminal Investigations Supervisors
Sent:	July 8, 2020 1:11:54 PM CDT
Received:	July 8, 2020 1:11:56 PM CDT

Fw: IACP's The Lead: Some US States Consider Police Licensing.

To: 2020 Criminal Investigations Supervisors, Mike Grimes
Sent: July 8, 2020 1:11:54 PM CDT
Received: July 8, 2020 1:12:04 PM CDT

Fw: IACP's The Lead: Some US States Consider Police Licensing.

To:	2020 Criminal Investigations Supervisors, Michael Dwyer (Sheriff)
Sent:	July 8, 2020 1:11:54 PM CDT
Received:	July 8, 2020 1:11:56 PM CDT

IACP's The Lead: Minnesota US Attorney Announces Task Force To Curb Gun Violence.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: jennifer.warren@cookcountyil.gov, Jennifer Warren (Sheriff) <jennifer.warren@cookcountyil.gov>

Sent: July 9, 2020 7:07:59 AM CDT
Received: July 9, 2020 7:08:13 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Jennifer Warren

Thursday, July 9, 2020

POLICING & POLICY

Minnesota US Attorney Announces Task Force To Curb Gun Violence

The Minneapolis Star Tribune (7/8) reports, "U.S. Attorney Erica MacDonald is mobilizing a multiagency command center for a new task force aimed at curbing "an extraordinary spike" in violence in the Twin Cities that has been on the rise since Memorial Day." MacDonald on Wednesday "outlined a 30-day operation that will deploy state and federal law enforcement across a dozen agencies in response to a spike in gun violence and other crimes."

The St. Paul (MN) Pioneer Press (7/8, Harville) reports, "The Twin Cities Violent Crime Task Force will work with additional state and federal resources to help local law enforcement investigate, arrest and prosecute individuals contributing to the gun violence in Minneapolis and St. Paul. As of Tuesday this year, 101 people have been shot in St. Paul, including some fatally, according to police. That's compared with 70 as of the end of June 2019. 'Law enforcement partners will utilize the task force to maximize intelligence gathering and information sharing capabilities to ensure swift and precise identification of those individuals who are perpetrating violence,' the U.S. Attorney's office said in a statement. MacDonald stressed that the goal of the task force is 'not to flood our communities with law enforcement,' but rather to create a way for community members and city leaders to collaborate with law enforcement while putting a stop to gun violence."

US Launches Anti-Crime Initiative In Kansas City, Missouri

The Washington Times (7/8, Boyer) reports the Administration is "surging federal law-enforcement agents into Kansas City, Missouri, to fight a wave of violent crime, the White House said Wednesday." Attorney General Barr is "launching the operation within the next 10 days with FBI agents, U.S. marshals, Drug Enforcement Administration agents and officials from the Bureau of Alcohol, Tobacco, Firearms and Explosives to help suppress what the White House called a 'tragic' rise in violence."

KCTV-TV Kansas City, MO (7/8, Smith) reports that "Operation: Legend" is "being touted by the Department of Justice as a response to the surge in violent crime in Kansas City. The focus of the new initiative is to increase the federal law enforcement present in the city. Press Secretary Kayleigh McEnany said the new plan was inspired by Mayor Quinton Lucas' letter to Missouri Governor Mike Parson where Lucas wrote that Kansas City was 'at a crisis point.' The letter, originally sent July 3, was looking for Parson to convene a special session of the Missouri legislature focused on growing crime in Missouri cities."

US Sen. Tim Scott Says Police Reform Bill Is Not Dead

The Washington Times (7/8, Mordock) reports Sen. Tim Scott (R-SC) said Wednesday a bill he authored on police reform "is not dead and he expects an agreement with the Democrat-controlled House in the next few weeks." Speaking with reporters at a press event with Attorney General Barr, "Scott said he has talked with House Democrats about reaching a deal." Said the senator, "Folks are now calling me about the legislation from the other side, suggesting perhaps it is not dead. We may have a Lazarus moment."

New Mexico Mandates Police Body Cameras

The AP (7/8) reports, "New Mexico will require that all state and local police officers wear body cameras in response to concern about excessive use of force by law enforcement, under a bill signed Wednesday by Gov. Michelle Lujan Grisham." The AP adds, "The reforms apply to local and state law enforcement officers with the exception of tribal governments. Law enforcement agencies must archive body camera footage for at least 120 days." The state legislature "approved the policing reforms during a four-day special session in June." The AP adds, "Police agencies that flout the new body-camera requirement can sued for withholding evidence."

Colorado City Passes Resolution Shielding Officers From Portion Of State Reform Law

The Denver Post (7/8, Aguilar) reports, "Just weeks after Colorado passed a sweeping police reform law, Greenwood Village has approved a measure that ensures its officers aren't on the hook financially if they mistreat or harm a citizen." Greenwood Village council members "unanimously passed a resolution Monday saying the city will never find its officers have acted in bad faith," and "that effectively shields them from having to face personal financial liability for misconduct on the job – contrary to a key stipulation of Senate Bill 217, which became law last month. 'The intent of Council's resolution was simply to inform its officers that as their employer, they would not make such a (bad-faith) finding no matter what,' Greenwood Village city attorney Tonya Haas Davidson wrote in an email Wednesday. 'Nowhere in the law is an employer ever required to make a finding of bad faith.'"

Chicago Police Announce Formation Of Citywide Unit To Fight Violent Crime

The Chicago Sun-Times (7/8) reports, "Chicago police announced Tuesday it will create a citywide violent crime unit after three consecutive weekends with at least 65 people shot and multiple children killed. The specialized unit is meant 'to tackle violent crime and create community partnerships in some of our most challenging areas,' the department said. 'The ultimate goal of the Chicago Police Department's organizational restructuring that began earlier this year has always been to bolster police resources under the authority of district commanders, while also being able to address spikes in violent crime citywide,' the department said." The Sun-Times adds, "Once implemented, the new unit will 'impact' gun, saturation and gang enforcement teams in each of the city's five police Areas, the department said. In the meantime, police are bolstering the Summer Mobile Patrol Unit, a task force of 100 officers focusing on high-crime areas."

After George Floyd's death and the response that followed, police leaders, community members, and elected officials in the United States and around the world are looking for collaborative, constructive ways to move public safety efforts forward. The IACP has launched a new Community-Police Engagement resource page featuring a variety of tools that provide policy considerations and tangible strategies to support police and communities in their efforts to engage in productive dialogue, form strong partnerships, and identify meaningful solutions. Topics include community policing; bias free policing; use of force; leadership and culture; and recruitment and promotional testing. At a time when agencies are looking to assess their policies and procedures and develop new initiatives to maximize community–police engagement, these tools provide a meaningful base to help public safety stakeholders develop a strong, consistent foundation.

Learn more.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Driver Charged With Vehicular Homicide In Death Of Seattle Protester

The Washington Post (7/8, Guarino) reports, "A man who allegedly struck Black Lives Matter protesters in Seattle with his car, killing one, was charged with reckless driving, vehicular assault and vehicular homicide by the King County Prosecuting Attorney's Office on Wednesday. Washington State Patrol and the FBI are investigating the case, a prominent and fatal example of recent car attacks on demonstrators." The Post adds, "When protesters gathered for a Black Femme March on Interstate 5 on July 3, it was the 19th consecutive night activists had done so, according to the state patrol. Near midnight, the patrol closed a section of the interstate for the demonstration. After 1 a.m., a white Jaguar, seen on security video entering the highway through an off-ramp, drove through the group at high speed, authorities said. The car struck two people – Summer Taylor, a 24-year-old Seattle resident, and Diaz Love, 32 – then fled the scene, speeding down the highway."

The New York Times (7/8, Waller, Paybarah) reports that Dawit Kelete, 27, "is being held with bail set at $1.2 million and is expected to remain in jail, the King County Prosecuting Attorney's Office said. Two of the charges, vehicular homicide and vehicular assault, are felonies, a spokesman for the prosecuting attorney's office said. Mr. Kelete could face more than 13 years in prison, said the spokesman, Casey McNerthney." The Times adds, "The Washington State Patrol and the F.B.I. were still investigating the matter, and Mr. Kelete could face additional charges, according to a statement from the prosecutor's office."

Crews Of ATM Thieves Using Trucks As Battering Rams Inside Baltimore, Maryland Businesses

The Baltimore Sun (7/8, Fenton) reports, "Sometimes, they operate with the speed and precision of a NASCAR pit crew – prying open the locked steel gates and doors of small businesses around Baltimore, then lifting away ATMs and hurrying them to a waiting pickup truck or van. Other times, the thieves use vehicles – typically stolen – as battering rams to force entry. They crash through storefronts to commit a small bank robbery that does not require holding up a teller." The Sun adds, "The chaotic crimes have continued on and off for months, with small businesses and one ATM distributor saying it's a new and alarming trend. During the course of one hour as the sun came up June 27, three stores were hit in west, northeast and midtown Baltimore, including someone ramming into a gas station on Moravia Road. They've used different methods and vehicles, causing police to believe it's not just the work of one crew and that others are getting in on the crime."

Mexican Drug Cartel Attacks Public Officials

The Wall Street Journal (7/8, Montes, de Córdoba, Subscription Publication) reports on the Jalisco New Generation Cartel, saying that it is the most important cartel in Mexico and has mounted direct assaults on Mexican officials and law enforcement. According to the Journal, the group is responsible for the deaths of over 100 officials. The US Drug Enforcement Administration is offering $10 million for information leading to the arrest of the group's leader Nemesio Oseguera.

WEDNESDAY'S LEAD STORIES

- **Some US States Consider Police Licensing**
- **Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests**
- **German Authorities Seize Server Hosting "BlueLeaks" Data Dump**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to jennifer.warren@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Minnesota US Attorney Announces Task Force To Curb Gun Violence.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: brian.white@cookcountyil.gov, Brian White (Sheriff) <Brian.White@cookcountyil.gov>

Sent: July 9, 2020 7:07:59 AM CDT
Received: July 9, 2020 7:08:14 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Brian White

Thursday, July 9, 2020

POLICING & POLICY

Minnesota US Attorney Announces Task Force To Curb Gun Violence

The Minneapolis Star Tribune (7/8) reports, "U.S. Attorney Erica MacDonald is mobilizing a multiagency command center for a new task force aimed at curbing "an extraordinary spike" in violence in the Twin Cities that has been on the rise since Memorial Day." MacDonald on Wednesday "outlined a 30-day operation that will deploy state and federal law enforcement across a dozen agencies in response to a spike in gun violence and other crimes."

The St. Paul (MN) Pioneer Press (7/8, Harville) reports, "The Twin Cities Violent Crime Task Force will work with additional state and federal resources to help local law enforcement investigate, arrest and prosecute individuals contributing to the gun violence in Minneapolis and St. Paul. As of Tuesday this year, 101 people have been shot in St. Paul, including some fatally, according to police. That's compared with 70 as of the end of June 2019. 'Law enforcement partners will utilize the task force to maximize intelligence gathering and information sharing capabilities to ensure swift and precise identification of those individuals who are perpetrating violence,' the U.S. Attorney's office said in a statement. MacDonald stressed that the goal of the task force is 'not to flood our communities with law enforcement,' but rather to create a way for community members and city leaders to collaborate with law enforcement while putting a stop to gun violence."

US Launches Anti-Crime Initiative In Kansas City, Missouri

The Washington Times (7/8, Boyer) reports the Administration is "surging federal law-enforcement agents into Kansas City, Missouri, to fight a wave of violent crime, the White House said Wednesday." Attorney General Barr is "launching the operation within the next 10 days with FBI agents, U.S. marshals, Drug Enforcement Administration agents and officials from the Bureau of Alcohol, Tobacco, Firearms and Explosives to help suppress what the White House called a 'tragic' rise in violence."

KCTV-TV Kansas City, MO (7/8, Smith) reports that "Operation: Legend" is "being touted by the Department of Justice as a response to the surge in violent crime in Kansas City. The focus of the new initiative is to increase the federal law enforcement present in the city. Press Secretary Kayleigh McEnany said the new plan was inspired by Mayor Quinton Lucas' letter to Missouri Governor Mike Parson where Lucas wrote that Kansas City was 'at a crisis point.' The letter, originally sent July 3, was looking for Parson to convene a special session of the Missouri legislature focused on growing crime in Missouri cities."

US Sen. Tim Scott Says Police Reform Bill Is Not Dead

The Washington Times (7/8, Mordock) reports Sen. Tim Scott (R-SC) said Wednesday a bill he authored on police reform "is not dead and he expects an agreement with the Democrat-controlled House in the next few weeks." Speaking with reporters at a press event with Attorney General Barr, "Scott said he has talked with House Democrats about reaching a deal." Said the senator, "Folks are now calling me about the legislation from the other side, suggesting perhaps it is not dead. We may have a Lazarus moment."

New Mexico Mandates Police Body Cameras

The AP (7/8) reports, "New Mexico will require that all state and local police officers wear body cameras in response to concern about excessive use of force by law enforcement, under a bill signed Wednesday by Gov. Michelle Lujan Grisham." The AP adds, "The reforms apply to local and state law enforcement officers with the exception of tribal governments. Law enforcement agencies must archive body camera footage for at least 120 days." The state legislature "approved the policing reforms during a four-day special session in June." The AP adds, "Police agencies that flout the new body-camera requirement can sued for withholding evidence."

Colorado City Passes Resolution Shielding Officers From Portion Of State Reform Law

The Denver Post (7/8, Aguilar) reports, "Just weeks after Colorado passed a sweeping police reform law, Greenwood Village has approved a measure that ensures its officers aren't on the hook financially if they mistreat or harm a citizen." Greenwood Village council members "unanimously passed a resolution Monday saying the city will never find its officers have acted in bad faith," and "that effectively shields them from having to face personal financial liability for misconduct on the job – contrary to a key stipulation of Senate Bill 217, which became law last month. 'The intent of Council's resolution was simply to inform its officers that as their employer, they would not make such a (bad-faith) finding no matter what,' Greenwood Village city attorney Tonya Haas Davidson wrote in an email Wednesday. 'Nowhere in the law is an employer ever required to make a finding of bad faith.'"

Chicago Police Announce Formation Of Citywide Unit To Fight Violent Crime

The Chicago Sun-Times (7/8) reports, "Chicago police announced Tuesday it will create a citywide violent crime unit after three consecutive weekends with at least 65 people shot and multiple children killed. The specialized unit is meant 'to tackle violent crime and create community partnerships in some of our most challenging areas,' the department said. 'The ultimate goal of the Chicago Police Department's organizational restructuring that began earlier this year has always been to bolster police resources under the authority of district commanders, while also being able to address spikes in violent crime citywide,' the department said." The Sun-Times adds, "Once implemented, the new unit will 'impact' gun, saturation and gang enforcement teams in each of the city's five police Areas, the department said. In the meantime, police are bolstering the Summer Mobile Patrol Unit, a task force of 100 officers focusing on high-crime areas."

After George Floyd's death and the response that followed, police leaders, community members, and elected officials in the United States and around the world are looking for collaborative, constructive ways to move public safety efforts forward. The IACP has launched a new Community-Police Engagement resource page featuring a variety of tools that provide policy considerations and tangible strategies to support police and communities in their efforts to engage in productive dialogue, form strong partnerships, and identify meaningful solutions. Topics include community policing; bias free policing; use of force; leadership and culture; and recruitment and promotional testing. At a time when agencies are looking to assess their policies and procedures and develop new initiatives to maximize community–police engagement, these tools provide a meaningful base to help public safety stakeholders develop a strong, consistent foundation.

Learn more.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Driver Charged With Vehicular Homicide In Death Of Seattle Protester

The Washington Post (7/8, Guarino) reports, "A man who allegedly struck Black Lives Matter protesters in Seattle with his car, killing one, was charged with reckless driving, vehicular assault and vehicular homicide by the King County Prosecuting Attorney's Office on Wednesday. Washington State Patrol and the FBI are investigating the case, a prominent and fatal example of recent car attacks on demonstrators." The Post adds, "When protesters gathered for a Black Femme March on Interstate 5 on July 3, it was the 19th consecutive night activists had done so, according to the state patrol. Near midnight, the patrol closed a section of the interstate for the demonstration. After 1 a.m., a white Jaguar, seen on security video entering the highway through an off-ramp, drove through the group at high speed, authorities said. The car struck two people – Summer Taylor, a 24-year-old Seattle resident, and Diaz Love, 32 – then fled the scene, speeding down the highway."

The New York Times (7/8, Waller, Paybarah) reports that Dawit Kelete, 27, "is being held with bail set at $1.2 million and is expected to remain in jail, the King County Prosecuting Attorney's Office said. Two of the charges, vehicular homicide and vehicular assault, are felonies, a spokesman for the prosecuting attorney's office said. Mr. Kelete could face more than 13 years in prison, said the spokesman, Casey McNerthney." The Times adds, "The Washington State Patrol and the F.B.I. were still investigating the matter, and Mr. Kelete could face additional charges, according to a statement from the prosecutor's office."

Crews Of ATM Thieves Using Trucks As Battering Rams Inside Baltimore, Maryland Businesses

The Baltimore Sun (7/8, Fenton) reports, "Sometimes, they operate with the speed and precision of a NASCAR pit crew – prying open the locked steel gates and doors of small businesses around Baltimore, then lifting away ATMs and hurrying them to a waiting pickup truck or van. Other times, the thieves use vehicles – typically stolen – as battering rams to force entry. They crash through storefronts to commit a small bank robbery that does not require holding up a teller." The Sun adds, "The chaotic crimes have continued on and off for months, with small businesses and one ATM distributor saying it's a new and alarming trend. During the course of one hour as the sun came up June 27, three stores were hit in west, northeast and midtown Baltimore, including someone ramming into a gas station on Moravia Road. They've used different methods and vehicles, causing police to believe it's not just the work of one crew and that others are getting in on the crime."

Mexican Drug Cartel Attacks Public Officials

The Wall Street Journal (7/8, Montes, de Córdoba, Subscription Publication) reports on the Jalisco New Generation Cartel, saying that it is the most important cartel in Mexico and has mounted direct assaults on Mexican officials and law enforcement. According to the Journal, the group is responsible for the deaths of over 100 officials. The US Drug Enforcement Administration is offering $10 million for information leading to the arrest of the group's leader Nemesio Oseguera.

WEDNESDAY'S LEAD STORIES

- **Some US States Consider Police Licensing**
- **Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests**
- **German Authorities Seize Server Hosting "BlueLeaks" Data Dump**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to brian.white@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Minnesota US Attorney Announces Task Force To Curb Gun Violence.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: keith.morrison@cookcountyil.gov, Keith Morrison (Sheriff) <Keith.Morrison@cookcountyil.gov>

Sent: July 9, 2020 7:07:59 AM CDT
Received: July 9, 2020 7:08:17 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Keith Morrison Thursday, July 9, 2020

POLICING & POLICY

Minnesota US Attorney Announces Task Force To Curb Gun Violence

The Minneapolis Star Tribune (7/8) reports, "U.S. Attorney Erica MacDonald is mobilizing a multiagency command center for a new task force aimed at curbing "an extraordinary spike" in violence in the Twin Cities that has been on the rise since Memorial Day." MacDonald on Wednesday "outlined a 30-day operation that will deploy state and federal law enforcement across a dozen agencies in response to a spike in gun violence and other crimes."

The St. Paul (MN) Pioneer Press (7/8, Harville) reports, "The Twin Cities Violent Crime Task Force will work with additional state and federal resources to help local law enforcement investigate, arrest and prosecute individuals contributing to the gun violence in Minneapolis and St. Paul. As of Tuesday this year, 101 people have been shot in St. Paul, including some fatally, according to police. That's compared with 70 as of the end of June 2019. 'Law enforcement partners will utilize the task force to maximize intelligence gathering and information sharing capabilities to ensure swift and precise identification of those individuals who are perpetrating violence,' the U.S. Attorney's office said in a statement. MacDonald stressed that the goal of the task force is 'not to flood our communities with law enforcement,' but rather to create a way for community members and city leaders to collaborate with law enforcement while putting a stop to gun violence."

US Launches Anti-Crime Initiative In Kansas City, Missouri

The Washington Times (7/8, Boyer) reports the Administration is "surging federal law-enforcement agents into Kansas City, Missouri, to fight a wave of violent crime, the White House said Wednesday." Attorney General Barr is "launching the operation within the next 10 days with FBI agents, U.S. marshals, Drug Enforcement Administration agents and officials from the Bureau of Alcohol, Tobacco, Firearms and Explosives to help suppress what the White House called a 'tragic' rise in violence."

KCTV-TV Kansas City, MO (7/8, Smith) reports that "Operation: Legend" is "being touted by the Department of Justice as a response to the surge in violent crime in Kansas City. The focus of the new initiative is to increase the federal law enforcement present in the city. Press Secretary Kayleigh McEnany said the new plan was inspired by Mayor Quinton Lucas' letter to Missouri Governor Mike Parson where Lucas wrote that Kansas City was 'at a crisis point.' The letter, originally sent July 3, was looking for Parson to convene a special session of the Missouri legislature focused on growing crime in Missouri cities."

US Sen. Tim Scott Says Police Reform Bill Is Not Dead

The Washington Times (7/8, Mordock) reports Sen. Tim Scott (R-SC) said Wednesday a bill he authored on police reform "is not dead and he expects an agreement with the Democrat-controlled House in the next few weeks." Speaking with reporters at a press event with Attorney General Barr, "Scott said he has talked with House Democrats about reaching a deal." Said the senator, "Folks are now calling me about the legislation from the other side, suggesting perhaps it is not dead. We may have a Lazarus moment."

New Mexico Mandates Police Body Cameras

The AP (7/8) reports, "New Mexico will require that all state and local police officers wear body cameras in response to concern about excessive use of force by law enforcement, under a bill signed Wednesday by Gov. Michelle Lujan Grisham." The AP adds, "The reforms apply to local and state law enforcement officers with the exception of tribal governments. Law enforcement agencies must archive body camera footage for at least 120 days." The state legislature "approved the policing reforms during a four-day special session in June." The AP adds, "Police agencies that flout the new body-camera requirement can sued for withholding evidence."

Colorado City Passes Resolution Shielding Officers From Portion Of State Reform Law

The Denver Post (7/8, Aguilar) reports, "Just weeks after Colorado passed a sweeping police reform law, Greenwood Village has approved a measure that ensures its officers aren't on the hook financially if they mistreat or harm a citizen." Greenwood Village council members "unanimously passed a resolution Monday saying the city will never find its officers have acted in bad faith," and "that effectively shields them from having to face personal financial liability for misconduct on the job – contrary to a key stipulation of Senate Bill 217, which became law last month. 'The intent of Council's resolution was simply to inform its officers that as their employer, they would not make such a (bad-faith) finding no matter what,' Greenwood Village city attorney Tonya Haas Davidson wrote in an email Wednesday. 'Nowhere in the law is an employer ever required to make a finding of bad faith.'"

Chicago Police Announce Formation Of Citywide Unit To Fight Violent Crime

The Chicago Sun-Times (7/8) reports, "Chicago police announced Tuesday it will create a citywide violent crime unit after three consecutive weekends with at least 65 people shot and multiple children killed. The specialized unit is meant 'to tackle violent crime and create community partnerships in some of our most challenging areas,' the department said. 'The ultimate goal of the Chicago Police Department's organizational restructuring that began earlier this year has always been to bolster police resources under the authority of district commanders, while also being able to address spikes in violent crime citywide,' the department said." The Sun-Times adds, "Once implemented, the new unit will 'impact' gun, saturation and gang enforcement teams in each of the city's five police Areas, the department said. In the meantime, police are bolstering the Summer Mobile Patrol Unit, a task force of 100 officers focusing on high-crime areas."

After George Floyd's death and the response that followed, police leaders, community members, and elected officials in the United States and around the world are looking for collaborative, constructive ways to move public safety efforts forward. The IACP has launched a new Community-Police Engagement resource page featuring a variety of tools that provide policy considerations and tangible strategies to support police and communities in their efforts to engage in productive dialogue, form strong partnerships, and identify meaningful solutions. Topics include community policing; bias free policing; use of force; leadership and culture; and recruitment and promotional testing. At a time when agencies are looking to assess their policies and procedures and develop new initiatives to maximize community–police engagement, these tools provide a meaningful base to help public safety stakeholders develop a strong, consistent foundation.

Learn more.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Driver Charged With Vehicular Homicide In Death Of Seattle Protester

The Washington Post (7/8, Guarino) reports, "A man who allegedly struck Black Lives Matter protesters in Seattle with his car, killing one, was charged with reckless driving, vehicular assault and vehicular homicide by the King County Prosecuting Attorney's Office on Wednesday. Washington State Patrol and the FBI are investigating the case, a prominent and fatal example of recent car attacks on demonstrators." The Post adds, "When protesters gathered for a Black Femme March on Interstate 5 on July 3, it was the 19th consecutive night activists had done so, according to the state patrol. Near midnight, the patrol closed a section of the interstate for the demonstration. After 1 a.m., a white Jaguar, seen on security video entering the highway through an off-ramp, drove through the group at high speed, authorities said. The car struck two people – Summer Taylor, a 24-year-old Seattle resident, and Diaz Love, 32 – then fled the scene, speeding down the highway."

The New York Times (7/8, Waller, Paybarah) reports that Dawit Kelete, 27, "is being held with bail set at $1.2 million and is expected to remain in jail, the King County Prosecuting Attorney's Office said. Two of the charges, vehicular homicide and vehicular assault, are felonies, a spokesman for the prosecuting attorney's office said. Mr. Kelete could face more than 13 years in prison, said the spokesman, Casey McNerthney." The Times adds, "The Washington State Patrol and the F.B.I. were still investigating the matter, and Mr. Kelete could face additional charges, according to a statement from the prosecutor's office."

Crews Of ATM Thieves Using Trucks As Battering Rams Inside Baltimore, Maryland Businesses

The Baltimore Sun (7/8, Fenton) reports, "Sometimes, they operate with the speed and precision of a NASCAR pit crew – prying open the locked steel gates and doors of small businesses around Baltimore, then lifting away ATMs and hurrying them to a waiting pickup truck or van. Other times, the thieves use vehicles – typically stolen – as battering rams to force entry. They crash through storefronts to commit a small bank robbery that does not require holding up a teller." The Sun adds, "The chaotic crimes have continued on and off for months, with small businesses and one ATM distributor saying it's a new and alarming trend. During the course of one hour as the sun came up June 27, three stores were hit in west, northeast and midtown Baltimore, including someone ramming into a gas station on Moravia Road. They've used different methods and vehicles, causing police to believe it's not just the work of one crew and that others are getting in on the crime."

Mexican Drug Cartel Attacks Public Officials

The Wall Street Journal (7/8, Montes, de Córdoba, Subscription Publication) reports on the Jalisco New Generation Cartel, saying that it is the most important cartel in Mexico and has mounted direct assaults on Mexican officials and law enforcement. According to the Journal, the group is responsible for the deaths of over 100 officials. The US Drug Enforcement Administration is offering $10 million for information leading to the arrest of the group's leader Nemesio Oseguera.

WEDNESDAY'S LEAD STORIES

- **Some US States Consider Police Licensing**
- **Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests**
- **German Authorities Seize Server Hosting "BlueLeaks" Data Dump**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to keith.morrison@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Minnesota US Attorney Announces Task Force To Curb Gun Violence.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: sean.gleason@cookcountyil.gov, Sean Gleason (Sheriff) <Sean.Gleason@cookcountyil.gov>

Sent: July 9, 2020 7:07:59 AM CDT
Received: July 9, 2020 7:08:15 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Sean Gleason

Thursday, July 9, 2020

POLICING & POLICY

Minnesota US Attorney Announces Task Force To Curb Gun Violence

The Minneapolis Star Tribune (7/8) reports, "U.S. Attorney Erica MacDonald is mobilizing a multiagency command center for a new task force aimed at curbing "an extraordinary spike" in violence in the Twin Cities that has been on the rise since Memorial Day." MacDonald on Wednesday "outlined a 30-day operation that will deploy state and federal law enforcement across a dozen agencies in response to a spike in gun violence and other crimes."

The St. Paul (MN) Pioneer Press (7/8, Harville) reports, "The Twin Cities Violent Crime Task Force will work with additional state and federal resources to help local law enforcement investigate, arrest and prosecute individuals contributing to the gun violence in Minneapolis and St. Paul. As of Tuesday this year, 101 people have been shot in St. Paul, including some fatally, according to police. That's compared with 70 as of the end of June 2019. 'Law enforcement partners will utilize the task force to maximize intelligence gathering and information sharing capabilities to ensure swift and precise identification of those individuals who are perpetrating violence,' the U.S. Attorney's office said in a statement. MacDonald stressed that the goal of the task force is 'not to flood our communities with law enforcement,' but rather to create a way for community members and city leaders to collaborate with law enforcement while putting a stop to gun violence."

US Launches Anti-Crime Initiative In Kansas City, Missouri

The Washington Times (7/8, Boyer) reports the Administration is "surging federal law-enforcement agents into Kansas City, Missouri, to fight a wave of violent crime, the White House said Wednesday." Attorney General Barr is "launching the operation within the next 10 days with FBI agents, U.S. marshals, Drug Enforcement Administration agents and officials from the Bureau of Alcohol, Tobacco, Firearms and Explosives to help suppress what the White House called a 'tragic' rise in violence."

KCTV-TV Kansas City, MO (7/8, Smith) reports that "Operation: Legend" is "being touted by the Department of Justice as a response to the surge in violent crime in Kansas City. The focus of the new initiative is to increase the federal law enforcement present in the city. Press Secretary Kayleigh McEnany said the new plan was inspired by Mayor Quinton Lucas' letter to Missouri Governor Mike Parson where Lucas wrote that Kansas City was 'at a crisis point.' The letter, originally sent July 3, was looking for Parson to convene a special session of the Missouri legislature focused on growing crime in Missouri cities."

US Sen. Tim Scott Says Police Reform Bill Is Not Dead

The Washington Times (7/8, Mordock) reports Sen. Tim Scott (R-SC) said Wednesday a bill he authored on police reform "is not dead and he expects an agreement with the Democrat-controlled House in the next few weeks." Speaking with reporters at a press event with Attorney General Barr, "Scott said he has talked with House Democrats about reaching a deal." Said the senator, "Folks are now calling me about the legislation from the other side, suggesting perhaps it is not dead. We may have a Lazarus moment."

New Mexico Mandates Police Body Cameras

The AP (7/8) reports, "New Mexico will require that all state and local police officers wear body cameras in response to concern about excessive use of force by law enforcement, under a bill signed Wednesday by Gov. Michelle Lujan Grisham." The AP adds, "The reforms apply to local and state law enforcement officers with the exception of tribal governments. Law enforcement agencies must archive body camera footage for at least 120 days." The state legislature "approved the policing reforms during a four-day special session in June." The AP adds, "Police agencies that flout the new body-camera requirement can sued for withholding evidence."

Colorado City Passes Resolution Shielding Officers From Portion Of State Reform Law

The Denver Post (7/8, Aguilar) reports, "Just weeks after Colorado passed a sweeping police reform law, Greenwood Village has approved a measure that ensures its officers aren't on the hook financially if they mistreat or harm a citizen." Greenwood Village council members "unanimously passed a resolution Monday saying the city will never find its officers have acted in bad faith," and "that effectively shields them from having to face personal financial liability for misconduct on the job – contrary to a key stipulation of Senate Bill 217, which became law last month. 'The intent of Council's resolution was simply to inform its officers that as their employer, they would not make such a (bad-faith) finding no matter what,' Greenwood Village city attorney Tonya Haas Davidson wrote in an email Wednesday. 'Nowhere in the law is an employer ever required to make a finding of bad faith.'"

Chicago Police Announce Formation Of Citywide Unit To Fight Violent Crime

The Chicago Sun-Times (7/8) reports, "Chicago police announced Tuesday it will create a citywide violent crime unit after three consecutive weekends with at least 65 people shot and multiple children killed. The specialized unit is meant 'to tackle violent crime and create community partnerships in some of our most challenging areas,' the department said. 'The ultimate goal of the Chicago Police Department's organizational restructuring that began earlier this year has always been to bolster police resources under the authority of district commanders, while also being able to address spikes in violent crime citywide,' the department said." The Sun-Times adds, "Once implemented, the new unit will 'impact' gun, saturation and gang enforcement teams in each of the city's five police Areas, the department said. In the meantime, police are bolstering the Summer Mobile Patrol Unit, a task force of 100 officers focusing on high-crime areas."

After George Floyd's death and the response that followed, police leaders, community members, and elected officials in the United States and around the world are looking for collaborative, constructive ways to move public safety efforts forward. The IACP has launched a new Community-Police Engagement resource page featuring a variety of tools that provide policy considerations and tangible strategies to support police and communities in their efforts to engage in productive dialogue, form strong partnerships, and identify meaningful solutions. Topics include community policing; bias free policing; use of force; leadership and culture; and recruitment and promotional testing. At a time when agencies are looking to assess their policies and procedures and develop new initiatives to maximize community–police engagement, these tools provide a meaningful base to help public safety stakeholders develop a strong, consistent foundation.

Learn more.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Driver Charged With Vehicular Homicide In Death Of Seattle Protester

The Washington Post (7/8, Guarino) reports, "A man who allegedly struck Black Lives Matter protesters in Seattle with his car, killing one, was charged with reckless driving, vehicular assault and vehicular homicide by the King County Prosecuting Attorney's Office on Wednesday. Washington State Patrol and the FBI are investigating the case, a prominent and fatal example of recent car attacks on demonstrators." The Post adds, "When protesters gathered for a Black Femme March on Interstate 5 on July 3, it was the 19th consecutive night activists had done so, according to the state patrol. Near midnight, the patrol closed a section of the interstate for the demonstration. After 1 a.m., a white Jaguar, seen on security video entering the highway through an off-ramp, drove through the group at high speed, authorities said. The car struck two people – Summer Taylor, a 24-year-old Seattle resident, and Diaz Love, 32 – then fled the scene, speeding down the highway."

The New York Times (7/8, Waller, Paybarah) reports that Dawit Kelete, 27, "is being held with bail set at $1.2 million and is expected to remain in jail, the King County Prosecuting Attorney's Office said. Two of the charges, vehicular homicide and vehicular assault, are felonies, a spokesman for the prosecuting attorney's office said. Mr. Kelete could face more than 13 years in prison, said the spokesman, Casey McNerthney." The Times adds, "The Washington State Patrol and the F.B.I. were still investigating the matter, and Mr. Kelete could face additional charges, according to a statement from the prosecutor's office."

Crews Of ATM Thieves Using Trucks As Battering Rams Inside Baltimore, Maryland Businesses

The Baltimore Sun (7/8, Fenton) reports, "Sometimes, they operate with the speed and precision of a NASCAR pit crew – prying open the locked steel gates and doors of small businesses around Baltimore, then lifting away ATMs and hurrying them to a waiting pickup truck or van. Other times, the thieves use vehicles – typically stolen – as battering rams to force entry. They crash through storefronts to commit a small bank robbery that does not require holding up a teller." The Sun adds, "The chaotic crimes have continued on and off for months, with small businesses and one ATM distributor saying it's a new and alarming trend. During the course of one hour as the sun came up June 27, three stores were hit in west, northeast and midtown Baltimore, including someone ramming into a gas station on Moravia Road. They've used different methods and vehicles, causing police to believe it's not just the work of one crew and that others are getting in on the crime."

Mexican Drug Cartel Attacks Public Officials

The Wall Street Journal (7/8, Montes, de Córdoba, Subscription Publication) reports on the Jalisco New Generation Cartel, saying that it is the most important cartel in Mexico and has mounted direct assaults on Mexican officials and law enforcement. According to the Journal, the group is responsible for the deaths of over 100 officials. The US Drug Enforcement Administration is offering $10 million for information leading to the arrest of the group's leader Nemesio Oseguera.

WEDNESDAY'S LEAD STORIES

- **Some US States Consider Police Licensing**
- **Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests**
- **German Authorities Seize Server Hosting "BlueLeaks" Data Dump**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to sean.gleason@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Minnesota US Attorney Announces Task Force To Curb Gun Violence.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: noureen.kapadia@cookcountyil.gov, Noureen Kapadia (Sheriff) <Noureen.Kapadia@cookcountyil.gov>

Sent: July 9, 2020 7:07:59 AM CDT
Received: July 9, 2020 7:08:17 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Noureen Kapadia Thursday, July 9, 2020

POLICING & POLICY

Minnesota US Attorney Announces Task Force To Curb Gun Violence

The Minneapolis Star Tribune (7/8) reports, "U.S. Attorney Erica MacDonald is mobilizing a multiagency command center for a new task force aimed at curbing "an extraordinary spike" in violence in the Twin Cities that has been on the rise since Memorial Day." MacDonald on Wednesday "outlined a 30-day operation that will deploy state and federal law enforcement across a dozen agencies in response to a spike in gun violence and other crimes."

The St. Paul (MN) Pioneer Press (7/8, Harville) reports, "The Twin Cities Violent Crime Task Force will work with additional state and federal resources to help local law enforcement investigate, arrest and prosecute individuals contributing to the gun violence in Minneapolis and St. Paul. As of Tuesday this year, 101 people have been shot in St. Paul, including some fatally, according to police. That's compared with 70 as of the end of June 2019. 'Law enforcement partners will utilize the task force to maximize intelligence gathering and information sharing capabilities to ensure swift and precise identification of those individuals who are perpetrating violence,' the U.S. Attorney's office said in a statement. MacDonald stressed that the goal of the task force is 'not to flood our communities with law enforcement,' but rather to create a way for community members and city leaders to collaborate with law enforcement while putting a stop to gun violence."

US Launches Anti-Crime Initiative In Kansas City, Missouri

The Washington Times (7/8, Boyer) reports the Administration is "surging federal law-enforcement agents into Kansas City, Missouri, to fight a wave of violent crime, the White House said Wednesday." Attorney General Barr is "launching the operation within the next 10 days with FBI agents, U.S. marshals, Drug Enforcement Administration agents and officials from the Bureau of Alcohol, Tobacco, Firearms and Explosives to help suppress what the White House called a 'tragic' rise in violence."

KCTV-TV Kansas City, MO (7/8, Smith) reports that "Operation: Legend" is "being touted by the Department of Justice as a response to the surge in violent crime in Kansas City. The focus of the new initiative is to increase the federal law enforcement present in the city. Press Secretary Kayleigh McEnany said the new plan was inspired by Mayor Quinton Lucas' letter to Missouri Governor Mike Parson where Lucas wrote that Kansas City was 'at a crisis point.' The letter, originally sent July 3, was looking for Parson to convene a special session of the Missouri legislature focused on growing crime in Missouri cities."

US Sen. Tim Scott Says Police Reform Bill Is Not Dead

The Washington Times (7/8, Mordock) reports Sen. Tim Scott (R-SC) said Wednesday a bill he authored on police reform "is not dead and he expects an agreement with the Democrat-controlled House in the next few weeks." Speaking with reporters at a press event with Attorney General Barr, "Scott said he has talked with House Democrats about reaching a deal." Said the senator, "Folks are now calling me about the legislation from the other side, suggesting perhaps it is not dead. We may have a Lazarus moment."

New Mexico Mandates Police Body Cameras

The AP (7/8) reports, "New Mexico will require that all state and local police officers wear body cameras in response to concern about excessive use of force by law enforcement, under a bill signed Wednesday by Gov. Michelle Lujan Grisham." The AP adds, "The reforms apply to local and state law enforcement officers with the exception of tribal governments. Law enforcement agencies must archive body camera footage for at least 120 days." The state legislature "approved the policing reforms during a four-day special session in June." The AP adds, "Police agencies that flout the new body-camera requirement can sued for withholding evidence."

Colorado City Passes Resolution Shielding Officers From Portion Of State Reform Law

The Denver Post (7/8, Aguilar) reports, "Just weeks after Colorado passed a sweeping police reform law, Greenwood Village has approved a measure that ensures its officers aren't on the hook financially if they mistreat or harm a citizen." Greenwood Village council members "unanimously passed a resolution Monday saying the city will never find its officers have acted in bad faith," and "that effectively shields them from having to face personal financial liability for misconduct on the job – contrary to a key stipulation of Senate Bill 217, which became law last month. 'The intent of Council's resolution was simply to inform its officers that as their employer, they would not make such a (bad-faith) finding no matter what,' Greenwood Village city attorney Tonya Haas Davidson wrote in an email Wednesday. 'Nowhere in the law is an employer ever required to make a finding of bad faith.'"

Chicago Police Announce Formation Of Citywide Unit To Fight Violent Crime

The Chicago Sun-Times (7/8) reports, "Chicago police announced Tuesday it will create a citywide violent crime unit after three consecutive weekends with at least 65 people shot and multiple children killed. The specialized unit is meant 'to tackle violent crime and create community partnerships in some of our most challenging areas,' the department said. 'The ultimate goal of the Chicago Police Department's organizational restructuring that began earlier this year has always been to bolster police resources under the authority of district commanders, while also being able to address spikes in violent crime citywide,' the department said." The Sun-Times adds, "Once implemented, the new unit will 'impact' gun, saturation and gang enforcement teams in each of the city's five police Areas, the department said. In the meantime, police are bolstering the Summer Mobile Patrol Unit, a task force of 100 officers focusing on high-crime areas."

After George Floyd's death and the response that followed, police leaders, community members, and elected officials in the United States and around the world are looking for collaborative, constructive ways to move public safety efforts forward. The IACP has launched a new Community-Police Engagement resource page featuring a variety of tools that provide policy considerations and tangible strategies to support police and communities in their efforts to engage in productive dialogue, form strong partnerships, and identify meaningful solutions. Topics include community policing; bias free policing; use of force; leadership and culture; and recruitment and promotional testing. At a time when agencies are looking to assess their policies and procedures and develop new initiatives to maximize community–police engagement, these tools provide a meaningful base to help public safety stakeholders develop a strong, consistent foundation.

Learn more.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Driver Charged With Vehicular Homicide In Death Of Seattle Protester

The Washington Post (7/8, Guarino) reports, "A man who allegedly struck Black Lives Matter protesters in Seattle with his car, killing one, was charged with reckless driving, vehicular assault and vehicular homicide by the King County Prosecuting Attorney's Office on Wednesday. Washington State Patrol and the FBI are investigating the case, a prominent and fatal example of recent car attacks on demonstrators." The Post adds, "When protesters gathered for a Black Femme March on Interstate 5 on July 3, it was the 19th consecutive night activists had done so, according to the state patrol. Near midnight, the patrol closed a section of the interstate for the demonstration. After 1 a.m., a white Jaguar, seen on security video entering the highway through an off-ramp, drove through the group at high speed, authorities said. The car struck two people – Summer Taylor, a 24-year-old Seattle resident, and Diaz Love, 32 – then fled the scene, speeding down the highway."

The New York Times (7/8, Waller, Paybarah) reports that Dawit Kelete, 27, "is being held with bail set at $1.2 million and is expected to remain in jail, the King County Prosecuting Attorney's Office said. Two of the charges, vehicular homicide and vehicular assault, are felonies, a spokesman for the prosecuting attorney's office said. Mr. Kelete could face more than 13 years in prison, said the spokesman, Casey McNerthney." The Times adds, "The Washington State Patrol and the F.B.I. were still investigating the matter, and Mr. Kelete could face additional charges, according to a statement from the prosecutor's office."

Crews Of ATM Thieves Using Trucks As Battering Rams Inside Baltimore, Maryland Businesses

The Baltimore Sun (7/8, Fenton) reports, "Sometimes, they operate with the speed and precision of a NASCAR pit crew – prying open the locked steel gates and doors of small businesses around Baltimore, then lifting away ATMs and hurrying them to a waiting pickup truck or van. Other times, the thieves use vehicles – typically stolen – as battering rams to force entry. They crash through storefronts to commit a small bank robbery that does not require holding up a teller." The Sun adds, "The chaotic crimes have continued on and off for months, with small businesses and one ATM distributor saying it's a new and alarming trend. During the course of one hour as the sun came up June 27, three stores were hit in west, northeast and midtown Baltimore, including someone ramming into a gas station on Moravia Road. They've used different methods and vehicles, causing police to believe it's not just the work of one crew and that others are getting in on the crime."

Mexican Drug Cartel Attacks Public Officials

The Wall Street Journal (7/8, Montes, de Córdoba, Subscription Publication) reports on the Jalisco New Generation Cartel, saying that it is the most important cartel in Mexico and has mounted direct assaults on Mexican officials and law enforcement. According to the Journal, the group is responsible for the deaths of over 100 officials. The US Drug Enforcement Administration is offering $10 million for information leading to the arrest of the group's leader Nemesio Oseguera.

WEDNESDAY'S LEAD STORIES

- **Some US States Consider Police Licensing**
- **Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests**
- **German Authorities Seize Server Hosting "BlueLeaks" Data Dump**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to noureen.kapadia@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Minnesota US Attorney Announces Task Force To Curb Gun Violence.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: thomas.conley@cookcountyil.gov, Thomas Conley (Sheriff) <Thomas.Conley@cookcountyil.gov>

Sent: July 9, 2020 7:07:59 AM CDT
Received: July 9, 2020 7:08:19 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Thomas Conley Thursday, July 9, 2020

POLICING & POLICY

Minnesota US Attorney Announces Task Force To Curb Gun Violence

The Minneapolis Star Tribune (7/8) reports, "U.S. Attorney Erica MacDonald is mobilizing a multiagency command center for a new task force aimed at curbing "an extraordinary spike" in violence in the Twin Cities that has been on the rise since Memorial Day." MacDonald on Wednesday "outlined a 30-day operation that will deploy state and federal law enforcement across a dozen agencies in response to a spike in gun violence and other crimes."

The St. Paul (MN) Pioneer Press (7/8, Harville) reports, "The Twin Cities Violent Crime Task Force will work with additional state and federal resources to help local law enforcement investigate, arrest and prosecute individuals contributing to the gun violence in Minneapolis and St. Paul. As of Tuesday this year, 101 people have been shot in St. Paul, including some fatally, according to police. That's compared with 70 as of the end of June 2019. 'Law enforcement partners will utilize the task force to maximize intelligence gathering and information sharing capabilities to ensure swift and precise identification of those individuals who are perpetrating violence,' the U.S. Attorney's office said in a statement. MacDonald stressed that the goal of the task force is 'not to flood our communities with law enforcement,' but rather to create a way for community members and city leaders to collaborate with law enforcement while putting a stop to gun violence."

US Launches Anti-Crime Initiative In Kansas City, Missouri

The Washington Times (7/8, Boyer) reports the Administration is "surging federal law-enforcement agents into Kansas City, Missouri, to fight a wave of violent crime, the White House said Wednesday." Attorney General Barr is "launching the operation within the next 10 days with FBI agents, U.S. marshals, Drug Enforcement Administration agents and officials from the Bureau of Alcohol, Tobacco, Firearms and Explosives to help suppress what the White House called a 'tragic' rise in violence."

KCTV-TV Kansas City, MO (7/8, Smith) reports that "Operation: Legend" is "being touted by the Department of Justice as a response to the surge in violent crime in Kansas City. The focus of the new initiative is to increase the federal law enforcement present in the city. Press Secretary Kayleigh McEnany said the new plan was inspired by Mayor Quinton Lucas' letter to Missouri Governor Mike Parson where Lucas wrote that Kansas City was 'at a crisis point.' The letter, originally sent July 3, was looking for Parson to convene a special session of the Missouri legislature focused on growing crime in Missouri cities."

US Sen. Tim Scott Says Police Reform Bill Is Not Dead

The Washington Times (7/8, Mordock) reports Sen. Tim Scott (R-SC) said Wednesday a bill he authored on police reform "is not dead and he expects an agreement with the Democrat-controlled House in the next few weeks." Speaking with reporters at a press event with Attorney General Barr, "Scott said he has talked with House Democrats about reaching a deal." Said the senator, "Folks are now calling me about the legislation from the other side, suggesting perhaps it is not dead. We may have a Lazarus moment."

New Mexico Mandates Police Body Cameras

The AP (7/8) reports, "New Mexico will require that all state and local police officers wear body cameras in response to concern about excessive use of force by law enforcement, under a bill signed Wednesday by Gov. Michelle Lujan Grisham." The AP adds, "The reforms apply to local and state law enforcement officers with the exception of tribal governments. Law enforcement agencies must archive body camera footage for at least 120 days." The state legislature "approved the policing reforms during a four-day special session in June." The AP adds, "Police agencies that flout the new body-camera requirement can sued for withholding evidence."

Colorado City Passes Resolution Shielding Officers From Portion Of State Reform Law

The Denver Post (7/8, Aguilar) reports, "Just weeks after Colorado passed a sweeping police reform law, Greenwood Village has approved a measure that ensures its officers aren't on the hook financially if they mistreat or harm a citizen." Greenwood Village council members "unanimously passed a resolution Monday saying the city will never find its officers have acted in bad faith," and "that effectively shields them from having to face personal financial liability for misconduct on the job – contrary to a key stipulation of Senate Bill 217, which became law last month. 'The intent of Council's resolution was simply to inform its officers that as their employer, they would not make such a (bad-faith) finding no matter what,' Greenwood Village city attorney Tonya Haas Davidson wrote in an email Wednesday. 'Nowhere in the law is an employer ever required to make a finding of bad faith.'"

Chicago Police Announce Formation Of Citywide Unit To Fight Violent Crime

The Chicago Sun-Times (7/8) reports, "Chicago police announced Tuesday it will create a citywide violent crime unit after three consecutive weekends with at least 65 people shot and multiple children killed. The specialized unit is meant 'to tackle violent crime and create community partnerships in some of our most challenging areas,' the department said. 'The ultimate goal of the Chicago Police Department's organizational restructuring that began earlier this year has always been to bolster police resources under the authority of district commanders, while also being able to address spikes in violent crime citywide,' the department said." The Sun-Times adds, "Once implemented, the new unit will 'impact' gun, saturation and gang enforcement teams in each of the city's five police Areas, the department said. In the meantime, police are bolstering the Summer Mobile Patrol Unit, a task force of 100 officers focusing on high-crime areas."

After George Floyd's death and the response that followed, police leaders, community members, and elected officials in the United States and around the world are looking for collaborative, constructive ways to move public safety efforts forward. The IACP has launched a new Community-Police Engagement resource page featuring a variety of tools that provide policy considerations and tangible strategies to support police and communities in their efforts to engage in productive dialogue, form strong partnerships, and identify meaningful solutions. Topics include community policing; bias free policing; use of force; leadership and culture; and recruitment and promotional testing. At a time when agencies are looking to assess their policies and procedures and develop new initiatives to maximize community–police engagement, these tools provide a meaningful base to help public safety stakeholders develop a strong, consistent foundation.

Learn more.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Driver Charged With Vehicular Homicide In Death Of Seattle Protester

The Washington Post (7/8, Guarino) reports, "A man who allegedly struck Black Lives Matter protesters in Seattle with his car, killing one, was charged with reckless driving, vehicular assault and vehicular homicide by the King County Prosecuting Attorney's Office on Wednesday. Washington State Patrol and the FBI are investigating the case, a prominent and fatal example of recent car attacks on demonstrators." The Post adds, "When protesters gathered for a Black Femme March on Interstate 5 on July 3, it was the 19th consecutive night activists had done so, according to the state patrol. Near midnight, the patrol closed a section of the interstate for the demonstration. After 1 a.m., a white Jaguar, seen on security video entering the highway through an off-ramp, drove through the group at high speed, authorities said. The car struck two people – Summer Taylor, a 24-year-old Seattle resident, and Diaz Love, 32 – then fled the scene, speeding down the highway."

The New York Times (7/8, Waller, Paybarah) reports that Dawit Kelete, 27, "is being held with bail set at $1.2 million and is expected to remain in jail, the King County Prosecuting Attorney's Office said. Two of the charges, vehicular homicide and vehicular assault, are felonies, a spokesman for the prosecuting attorney's office said. Mr. Kelete could face more than 13 years in prison, said the spokesman, Casey McNerthney." The Times adds, "The Washington State Patrol and the F.B.I. were still investigating the matter, and Mr. Kelete could face additional charges, according to a statement from the prosecutor's office."

Crews Of ATM Thieves Using Trucks As Battering Rams Inside Baltimore, Maryland Businesses

The Baltimore Sun (7/8, Fenton) reports, "Sometimes, they operate with the speed and precision of a NASCAR pit crew – prying open the locked steel gates and doors of small businesses around Baltimore, then lifting away ATMs and hurrying them to a waiting pickup truck or van. Other times, the thieves use vehicles – typically stolen – as battering rams to force entry. They crash through storefronts to commit a small bank robbery that does not require holding up a teller." The Sun adds, "The chaotic crimes have continued on and off for months, with small businesses and one ATM distributor saying it's a new and alarming trend. During the course of one hour as the sun came up June 27, three stores were hit in west, northeast and midtown Baltimore, including someone ramming into a gas station on Moravia Road. They've used different methods and vehicles, causing police to believe it's not just the work of one crew and that others are getting in on the crime."

Mexican Drug Cartel Attacks Public Officials

The Wall Street Journal (7/8, Montes, de Córdoba, Subscription Publication) reports on the Jalisco New Generation Cartel, saying that it is the most important cartel in Mexico and has mounted direct assaults on Mexican officials and law enforcement. According to the Journal, the group is responsible for the deaths of over 100 officials. The US Drug Enforcement Administration is offering $10 million for information leading to the arrest of the group's leader Nemesio Oseguera.

WEDNESDAY'S LEAD STORIES

- **Some US States Consider Police Licensing**
- **Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests**
- **German Authorities Seize Server Hosting "BlueLeaks" Data Dump**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to thomas.conley@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Minnesota US Attorney Announces Task Force To Curb Gun Violence.

From: The IACP <TheLead@iacp.bulletinmedia.com>
To: theresa.olson@cookcountyil.gov, Theresa Olson (Sheriff) <Theresa.Olson@cookcountyil.gov>

Sent: July 9, 2020 7:07:59 AM CDT
Received: July 9, 2020 7:08:16 AM CDT

External Message Disclaimer

This message originated from an external source. Please use proper judgment and caution when opening attachments, clicking links, or responding to this email.

If you are unable to see the message or images below, click here to view

Greetings Theresa Olson

Thursday, July 9, 2020

POLICING & POLICY

Minnesota US Attorney Announces Task Force To Curb Gun Violence

The Minneapolis Star Tribune (7/8) reports, "U.S. Attorney Erica MacDonald is mobilizing a multiagency command center for a new task force aimed at curbing "an extraordinary spike" in violence in the Twin Cities that has been on the rise since Memorial Day." MacDonald on Wednesday "outlined a 30-day operation that will deploy state and federal law enforcement across a dozen agencies in response to a spike in gun violence and other crimes."

The St. Paul (MN) Pioneer Press (7/8, Harville) reports, "The Twin Cities Violent Crime Task Force will work with additional state and federal resources to help local law enforcement investigate, arrest and prosecute individuals contributing to the gun violence in Minneapolis and St. Paul. As of Tuesday this year, 101 people have been shot in St. Paul, including some fatally, according to police. That's compared with 70 as of the end of June 2019. 'Law enforcement partners will utilize the task force to maximize intelligence gathering and information sharing capabilities to ensure swift and precise identification of those individuals who are perpetrating violence,' the U.S. Attorney's office said in a statement. MacDonald stressed that the goal of the task force is 'not to flood our communities with law enforcement,' but rather to create a way for community members and city leaders to collaborate with law enforcement while putting a stop to gun violence."

US Launches Anti-Crime Initiative In Kansas City, Missouri

The Washington Times (7/8, Boyer) reports the Administration is "surging federal law-enforcement agents into Kansas City, Missouri, to fight a wave of violent crime, the White House said Wednesday." Attorney General Barr is "launching the operation within the next 10 days with FBI agents, U.S. marshals, Drug Enforcement Administration agents and officials from the Bureau of Alcohol, Tobacco, Firearms and Explosives to help suppress what the White House called a 'tragic' rise in violence."

KCTV-TV Kansas City, MO (7/8, Smith) reports that "Operation: Legend" is "being touted by the Department of Justice as a response to the surge in violent crime in Kansas City. The focus of the new initiative is to increase the federal law enforcement present in the city. Press Secretary Kayleigh McEnany said the new plan was inspired by Mayor Quinton Lucas' letter to Missouri Governor Mike Parson where Lucas wrote that Kansas City was 'at a crisis point.' The letter, originally sent July 3, was looking for Parson to convene a special session of the Missouri legislature focused on growing crime in Missouri cities."

US Sen. Tim Scott Says Police Reform Bill Is Not Dead

The Washington Times (7/8, Mordock) reports Sen. Tim Scott (R-SC) said Wednesday a bill he authored on police reform "is not dead and he expects an agreement with the Democrat-controlled House in the next few weeks." Speaking with reporters at a press event with Attorney General Barr, "Scott said he has talked with House Democrats about reaching a deal." Said the senator, "Folks are now calling me about the legislation from the other side, suggesting perhaps it is not dead. We may have a Lazarus moment."

New Mexico Mandates Police Body Cameras

The AP (7/8) reports, "New Mexico will require that all state and local police officers wear body cameras in response to concern about excessive use of force by law enforcement, under a bill signed Wednesday by Gov. Michelle Lujan Grisham." The AP adds, "The reforms apply to local and state law enforcement officers with the exception of tribal governments. Law enforcement agencies must archive body camera footage for at least 120 days." The state legislature "approved the policing reforms during a four-day special session in June." The AP adds, "Police agencies that flout the new body-camera requirement can sued for withholding evidence."

Colorado City Passes Resolution Shielding Officers From Portion Of State Reform Law

The Denver Post (7/8, Aguilar) reports, "Just weeks after Colorado passed a sweeping police reform law, Greenwood Village has approved a measure that ensures its officers aren't on the hook financially if they mistreat or harm a citizen." Greenwood Village council members "unanimously passed a resolution Monday saying the city will never find its officers have acted in bad faith," and "that effectively shields them from having to face personal financial liability for misconduct on the job – contrary to a key stipulation of Senate Bill 217, which became law last month. 'The intent of Council's resolution was simply to inform its officers that as their employer, they would not make such a (bad-faith) finding no matter what,' Greenwood Village city attorney Tonya Haas Davidson wrote in an email Wednesday. 'Nowhere in the law is an employer ever required to make a finding of bad faith.'"

Chicago Police Announce Formation Of Citywide Unit To Fight Violent Crime

The Chicago Sun-Times (7/8) reports, "Chicago police announced Tuesday it will create a citywide violent crime unit after three consecutive weekends with at least 65 people shot and multiple children killed. The specialized unit is meant 'to tackle violent crime and create community partnerships in some of our most challenging areas,' the department said. 'The ultimate goal of the Chicago Police Department's organizational restructuring that began earlier this year has always been to bolster police resources under the authority of district commanders, while also being able to address spikes in violent crime citywide,' the department said." The Sun-Times adds, "Once implemented, the new unit will 'impact' gun, saturation and gang enforcement teams in each of the city's five police Areas, the department said. In the meantime, police are bolstering the Summer Mobile Patrol Unit, a task force of 100 officers focusing on high-crime areas."

After George Floyd's death and the response that followed, police leaders, community members, and elected officials in the United States and around the world are looking for collaborative, constructive ways to move public safety efforts forward. The IACP has launched a new Community-Police Engagement resource page featuring a variety of tools that provide policy considerations and tangible strategies to support police and communities in their efforts to engage in productive dialogue, form strong partnerships, and identify meaningful solutions. Topics include community policing; bias free policing; use of force; leadership and culture; and recruitment and promotional testing. At a time when agencies are looking to assess their policies and procedures and develop new initiatives to maximize community–police engagement, these tools provide a meaningful base to help public safety stakeholders develop a strong, consistent foundation.

Learn more.

Connect with the IACP online:

IACP Event Calendar:

CRIME & DRUGS

Driver Charged With Vehicular Homicide In Death Of Seattle Protester

The Washington Post (7/8, Guarino) reports, "A man who allegedly struck Black Lives Matter protesters in Seattle with his car, killing one, was charged with reckless driving, vehicular assault and vehicular homicide by the King County Prosecuting Attorney's Office on Wednesday. Washington State Patrol and the FBI are investigating the case, a prominent and fatal example of recent car attacks on demonstrators." The Post adds, "When protesters gathered for a Black Femme March on Interstate 5 on July 3, it was the 19th consecutive night activists had done so, according to the state patrol. Near midnight, the patrol closed a section of the interstate for the demonstration. After 1 a.m., a white Jaguar, seen on security video entering the highway through an off-ramp, drove through the group at high speed, authorities said. The car struck two people – Summer Taylor, a 24-year-old Seattle resident, and Diaz Love, 32 – then fled the scene, speeding down the highway."

The New York Times (7/8, Waller, Paybarah) reports that Dawit Kelete, 27, "is being held with bail set at $1.2 million and is expected to remain in jail, the King County Prosecuting Attorney's Office said. Two of the charges, vehicular homicide and vehicular assault, are felonies, a spokesman for the prosecuting attorney's office said. Mr. Kelete could face more than 13 years in prison, said the spokesman, Casey McNerthney." The Times adds, "The Washington State Patrol and the F.B.I. were still investigating the matter, and Mr. Kelete could face additional charges, according to a statement from the prosecutor's office."

Crews Of ATM Thieves Using Trucks As Battering Rams Inside Baltimore, Maryland Businesses

The Baltimore Sun (7/8, Fenton) reports, "Sometimes, they operate with the speed and precision of a NASCAR pit crew – prying open the locked steel gates and doors of small businesses around Baltimore, then lifting away ATMs and hurrying them to a waiting pickup truck or van. Other times, the thieves use vehicles – typically stolen – as battering rams to force entry. They crash through storefronts to commit a small bank robbery that does not require holding up a teller." The Sun adds, "The chaotic crimes have continued on and off for months, with small businesses and one ATM distributor saying it's a new and alarming trend. During the course of one hour as the sun came up June 27, three stores were hit in west, northeast and midtown Baltimore, including someone ramming into a gas station on Moravia Road. They've used different methods and vehicles, causing police to believe it's not just the work of one crew and that others are getting in on the crime."

Mexican Drug Cartel Attacks Public Officials

The Wall Street Journal (7/8, Montes, de Córdoba, Subscription Publication) reports on the Jalisco New Generation Cartel, saying that it is the most important cartel in Mexico and has mounted direct assaults on Mexican officials and law enforcement. According to the Journal, the group is responsible for the deaths of over 100 officials. The US Drug Enforcement Administration is offering $10 million for information leading to the arrest of the group's leader Nemesio Oseguera.

WEDNESDAY'S LEAD STORIES

- **Some US States Consider Police Licensing**
- **Black Americans Report Hate Crimes, Violence In Wake Of Floyd Protests**
- **German Authorities Seize Server Hosting "BlueLeaks" Data Dump**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to theresa.olson@cookcountyil.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

IACP's The Lead: Minnesota US Attorney Announces Task Force To Curb Gun Violence.

To: Jennifer Warren (Sheriff)
Sent: July 9, 2020 7:07:59 AM CDT
Received: July 9, 2020 7:08:13 AM CDT

IACP's The Lead: Minnesota US Attorney Announces Task Force To Curb Gun Violence.

To:	Brian White (Sheriff), Abraham Yasin (Sheriff), Tarry Williams (Sheriff), Leo Schmitz (Sheriff), Adriana Morales (Sheriff), Alfonzo Hunter (Sheriff), Amanda Gallegos (Sheriff), Amar Patel (Sheriff), Bradley Curry (Sheriff), Carmen Gercone (Sheriff), Carmen Ruffin (Sheriff), Christopher Imhof (Sheriff), David Chiko (Sheriff), Erik Roedel (Sheriff), Gregory Ernst (Sheriff), Heather Bock (Sheriff), Jennifer Black (Sheriff), Jerry Baldwin (Sheriff), John Vega (Sheriff), John Webb (Sheriff), Jonathan Myslinski (Sheriff), Joseph Bellettiere (Sheriff), Kathleen Urbanczyk (Sheriff), Kelley Eldridge (Sheriff), Kevin Connelly (Sheriff), Kevin Ruel (Sheriff), Larry Schurig (Sheriff), Lonnie Hollis (Sheriff), Marlon Parks (Sheriff), Matthew Creen (Sheriff), Michael Brady (Sheriff), Michael Lucente (Sheriff), Michael Miller (Sheriff), Patrick Dwyer (Sheriff), Patrick Moerlien (Sheriff), Richard Brogan (Sheriff), Richard O'Brien (Sheriff), Robert Lunk (Sheriff), Ronald Jenkins (Sheriff), Stephen Bouffard (Sheriff), Theodore Stajura (Sheriff), Jason Hernandez (Sheriff), James Moore (Sheriff), Arunas Buntinas (Sheriff)
Cc:	Bradley Curry (Sheriff), Marlon Parks (Sheriff), Brian White (Sheriff), Arunas Buntinas (Sheriff), Tarry Williams (Sheriff)
Sent:	July 9, 2020 7:07:59 AM CDT
Received:	July 9, 2020 7:08:14 AM CDT

IACP's The Lead: Minnesota US Attorney Announces Task Force To Curb Gun Violence.

To:	Sean Gleason (Sheriff)
Sent:	July 9, 2020 7:07:59 AM CDT
Received:	July 9, 2020 7:08:15 AM CDT

IACP's The Lead: Minnesota US Attorney Announces Task Force To Curb Gun Violence.

To: Noureen Kapadia (Sheriff)
Sent: July 9, 2020 7:07:59 AM CDT
Received: July 9, 2020 7:08:18 AM CDT

IACP's The Lead: Minnesota US Attorney Announces Task Force To Curb Gun Violence.

To:	Thomas Conley (Sheriff)
Sent:	July 9, 2020 7:07:59 AM CDT
Received:	July 9, 2020 7:08:19 AM CDT

IACP's The Lead: Minnesota US Attorney Announces Task Force To Curb Gun Violence.

To: Theresa Olson (Sheriff)
Sent: July 9, 2020 7:07:59 AM CDT
Received: July 9, 2020 7:08:17 AM CDT